CUK-H02707-72-P014918

AMERICAN
JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

72

EDITED BY

WEI-LIANG CHOW
THE JOHNS HOPKINS UNIVERSITY

J. A. DIEUDONNÉ
NORTHWESTERN UNIVERSITY

A. M. GLEASON
HARVARD UNIVERSITY

PHILIP HARTMAN
THE JOHNS HOPKINS UNIVERSITY

WITH THE COÖPERATION OF

L. V. AHLFORS
A. BOREL
H. CARTAN
S. S. CHERN
C. CHEVALLEY
K. IWASAWA
K. KODAIRA
F. I. MAUTNER
J. MILNOR
A. WEIL

PUBLISHED UNDER THE JOINT AUSPICES OF
THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

51 [illegible]

VOLUME LXXX

1958

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

7/8

P14718

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

INDEX

PAGE

Anderson, R. D. The algebraic simplicity of certain groups of homeomorphisms, ... 955

Andreotti, Aldo. On a theorem of Torelli, ... 801

Aurora, Silvio. On power multiplicative norms, ... 879

Baily, Walter L., Jr. Satake's compactification of V_n, . . 348

Barcus, W. D. and J.-P. Meyer. The suspension of a loop space, . 895

Brauer, Fred and Shlomo Sternberg. Local uniqueness, existence in the large, and the convergence of successive approximations, 421

Berberian, S. K. $N \times N$ matrices over an AW^*-algebra, . . 37

Borel, A. and F. Hirzebruch. Characteristic classes and homogeneous spaces, I, ... 458

Bott, Raoul and Hans Samelson. Applications of the theory of Morse to symmetric spaces, ... 964

Browder, Felix E. Eigenfunction expansions for non-symmetric partial differential operators, I, ... 365

Calderón, A. P. Uniqueness in the Cauchy problem for partial differential equations, ... 16

Carleson, Lennart. An interpolation problem for bounded analytic functions, ... 921

Cartier, P. et J. Dixmier. Vecteurs analytiques dans les représentations de groupes de Lie, ... 131

Chow, Wei-Liang. Remarks on my paper "The Jacobian variety of an algebraic curve, ... 238

Chow, Wei-Liang. The criterion for unit multiplicity and a generalization of Hensel's lemma, ... 539

Corson, H. H. The determination of paracompactness by uniformities, ... 185

Devinatz, A. and I. I. Hirschman, Jr. The spectra of multiplier transforms on l^p, ... 829

Dieudonné, Jean. Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, ... 740

Dixmier, J. See P. Cartier et J. Dixmier, page 131.

PAGE

GERSTENHABER, MURRAY. On nilalgebras and linear varieties of nilpotent matrices, I, ... 614

HARISH-CHANDRA. Spherical functions on a semisimple Lie group, I, 241

HARISH-CHANDRA. Spherical functions on a semisimple Lie group, II, 553

HIRSCHMAN, I. I., JR. See A. Devinatz and I. I. Hirschman, Jr., page 829.

HIRZEBRUCH, F. See A. Borel and F. Hirzebruch, page 458.

IN MEMORIAM. Aurel Wintner, 1903-1958, ... 1

IWASAWA, KENKICHI. On some invariants of cyclotomic fields, . 773

KERVAIRE, MICHEL. On the Pontryagin classes of certain $\boldsymbol{SO}(n)$, bundles over manifolds, ... 632

KOLCHIN, ELLIS and SERGE LANG. Algebraic groups and the Galois theory of differential fields, ... 103

LANG, SERGE. See Ellis Kolchin and Serge Lang, page 103.

LANG, SERGE. Reciprocity and correspondences, ... 431

LANG, SERGE and JOHN TATE. Principal homogeneous spaces over Abelian varieties, ... 659

MATSUSAKA, T. Polarized varieties, fields of moduli and generalized Kummer varieties of polarized Abelian varieties, . . 45

MATSUSAKA, T. On a theorem of Torelli, ... 784

MAUTNER, F. I. Spherical functions over $\mathfrak{P}$-adic fields, I, . . 441

MEYER, J.-P. See W. D. Barcus and J.-P. Meyer, page 895.

MORREY, CHARLES B., JR. On the analyticity of the solutions of analytic non-linear elliptic systems of partial differential equations. Part I, ... 198

MORREY, CHARLES B., JR. On the analyticity of the solutions of analytic non-linear elliptic systems of partial differential equations. Part II, ... 219

MURRE, J. P. On a connectedness theorem for a birational transformation at a simple point, ... 3

MURRE, J. P. Intersection multiplicites of maximal connected bunches, 311

MOSTOW, G. D. Extensions of representations of Lie groups, II, . 331

NAGATA, MASAYOSHI. A general theory of algebraic geometry over Dedekind domains, II, ... 382

NASH, J. Continuity of solutions of parabolic and elliptic equations, 931

PAGE

O'Meara, O. T. The integral representations of quadratic forms over local fields, ... 843

Rosenlicht, Maxwell. Extensions of vector groups by Abelian varieties, ... 685

Samelson, Hans. See Raoul Bott and Hans Samelson, page 964.

Schlesinger, Ernest C. Conformal invariants and prime ends, . 83

Serre, Jean-Pierre. Quelques propriétés des variétés abéliennes en en caractéristique p, ... 715

Sternberg, Shlomo. See Fred Brauer and Shlomo Sternberg, page 421.

Sternberg, Shlomo. On the structure of local homeomorphisms of Euclidean n-space, II, ... 623

Tamagawa, Tsuneo. On the structure of orthogonal groups, . . 191

Tate, John. See Serge Lang and John Tate, page 659.

Wintner, Aurel. Stratifications of Cauchy's "stable" transcendents of Mittag-Leffler's entire functions, ... 111

Wintner, Aurel. On cosine-like arches, ... 125

Wintner, Aurel. In the λ-variant of Mertens' μ-hypothesis, . . 639

Wright, E. M. Partitions of large bipartites, ... 643

Zariski, Oscar. The problem of minimal models in the theory of algebraic surfaces, ... 146

CALCUTTA UNIVERSITY
CENTRAL LIBRARY

AUREL WINTNER, 1903-1958.

With deep sorrow we announce the sudden and premature death of our colleague, Aurel Wintner, on January 15, 1958.

Aurel Wintner was born in Budapest on April 8, 1903. He studied mathematics and astronomy at the University of Leipzig. During that period he was editorial assistant for the *Mathematische Zeitschrift* under Leon Lichtenstein, who was then, and for many years, chief editor of that journal; this period of apprenticeship had a profound influence on him, and he always preserved a deep sense of gratitude to the man under whom he had served. He took his Ph. D. in Leipzig in 1929, and then spent one semester in Rome as a fellow of the Rockefeller Foundation and another in Copenhagen, where he worked with E. Strömgren. In 1929 he published in Leipzig the book "Spektraltheorie der unendlichen Matrizen," which established his reputation as a mathematician. It was in Copenhagen that, in the year 1930, he married the daughter of Otto Hölder, one of his Leipzig teachers. In 1930 he came to the United States to join the faculty of The Johns Hopkins University, where he remained until his death. In the year 1944 he became one of the editors of this Journal, to which he devoted the best part of his energy, both by his scientific contributions (a substantial part of his most valuable work since he came to America was published there) and as an editor. For many years he was the mainspring of the *American Journal of Mathematics*. In a very real sense, he was the Journal.

THE EDITORS

ON A CONNECTEDNESS THEOREM FOR A BIRATIONAL TRANSFORMATION AT A SIMPLE POINT.*

By J. P. MURRE.[1]

Introduction. In 1951, Zariski obtained as a special case of his connectedness theorems the fact that the total transform of a normal point by a birational transformation is connected [III]. In a recent paper, [IV], the connectedness of the total transform of a simple point by a birational transformation is proved without using the theory of holomorphic functions developed in [III].

In this paper another proof is obtained of this connectedness-theorem for a birational transformation at a simple point. In fact, a somewhat stronger result is proved, namely, the following. Chow has introduced the concept of *linear connectedness*, a set is said to be linearly connected if every pair of points can be connected by a sequence of rational curves in that set. In this sense, the total transform of a simple point by a birational transformation is linearly connected.[2]

Furthermore, some applications are derived for specializations of a complete set of conjugates over a purely transcendental function field.

The terminology and notations are from [I].

In conclusion, I want to express my warmest thanks to Professor A. Weil and Professor T. Matsusaka for their advice and interest during the preparation of this paper. I am especially indebted to Professor Weil for suggestions which improve the exposition of the proof of Theorem 1.

1. The connectedness of the total transform of a point by a birational transformation of n-space.

Let V be an (abstract) variety and let $\mathfrak{B}$ be a

---

* Received December 15, 1956; revised July 29, 1957.

[1] This paper is the first part of a thesis presented to the University of Leyden in The Netherlands in fulfillment of the requirements for the Ph. D. examination. The paper was prepared while the author was working at the University of Chicago as a participant of the I. C. A. Scientists Research Project TA-01-101-3006.

[2] I am indebted to Professor Chow for calling my attention to the fact that the original proof implicitly contained this result. He also gave as an example a cubic cone, which shows that the assumption of a simple point is essential for this linearity property.

bunch of subvarieties of V. The point set attached to $\mathfrak{B}$ will be denoted by $\{\mathfrak{B}\}$. $\mathfrak{B}$ is called *connected* when it is not possible to divide the components of $\mathfrak{B}$ into two new bunches $\mathfrak{C}$ and $\mathfrak{D}$ such that $\{\mathfrak{B}\} = \{\mathfrak{C}\} \cup \{\mathfrak{D}\}$ and $\{\mathfrak{C}\} \cap \{\mathfrak{D}\} = \phi$. An equivalent definition for connectedness is the following. Let K be a field over which all the components of $\mathfrak{B}$ are defined and suppose Q and Q' are arbitrary points of $\{\mathfrak{B}\}$, then there exists a sequence of points in $\{\mathfrak{B}\}$, $Q = P_1, P_2, \cdots, P_{2n+1} = Q'$, such that $P_{2i} \rightarrow P_{2i-1}$ and $P_{2i} \rightarrow P_{2i+1}$ over K for $i = 1, 2, \cdots, n$. The above sequence is called a *connecting sequence* in $\mathfrak{B}$ between Q and Q'. More geometrically, $\mathfrak{B}$ is connected if and only if it is possible to connect two arbitrary points in $\{\mathfrak{B}\}$ by curves in $\{\mathfrak{B}\}$. (This follows, for instance, from [II], Lemma 7.) The concept of connectedness can also be obtained by introducing the Zariski-topology on V and then employing the usual definition of connectedness in this topology. Further two points are said to be *linearly connected in* $\mathfrak{B}$ if there exists a sequence of *rational* curves in $\{\mathfrak{B}\}$ connecting them, and $\mathfrak{B}$ is said to be *linearly connected* if every pair of its points are linearly connected in $\mathfrak{B}$.

Suppose U and V are varieties; let W be a subvariety of $U \times V$ and let Q be a point of U. If there is any component in $W \cap (Q \times V)$ then this component is of the form $Q \times Z$, ([I], Chap. IV, Cor. 6 of Th. 6), where Z is a subvariety of V. The bunch $W\{Q\}$, the *total transform* of Q by W, is defined as follows: $W \cap (Q \times V) = Q \times W\{Q\}$.

To prove the connectedness theorem, we first prove a—rather formal—lemma.

LEMMA.[3] *Let* $f_0, f_1, \cdots, f_m$ *be* $m + 1$ *polynomials in the indeterminates* $V_1, \cdots, V_h$ *and* Z *with coefficients in a field* k. *Let* $v_1, \cdots, v_h$ *and* z *be* $h + 1$ *elements of the ring* $k[[T]]$ *such that the* $f_i(v, 0)$ *are not all* 0 *and the* $f_i(v, z)$ *are not all* 0. *Then there is a field* $K \supset k$ *and an integer* $N > 0$ *and elements* z_j $(j = 0, 1, \cdots, 2n;\ z_0 = z,\ z_{2n} = 0)$ *in the ring* $K[[T^{1/N}]]$, *with the following properties. For each* j, *not all the* $f_i(v, z_j)$ *are* 0, *and if we denote by* R_j *the point in projective m-space obtained by putting* $T = 0$ *in the ratios of the homogeneous coordinates of the point* $[f_0(v, z_j), \cdots, f_m(v, z_j)]$, *then for every triple* $(2q, 2q + 1, 2q + 2)$, *where* $q = 0, 1, \cdots, n - 1$, *either* $R_{2q} = R_{2q+1} = R_{2q+2}$ *or there exists a rational curve* C_q *having, over a suitable field containing* k, *the point* R_{2q+1} *as a generic point and going through* R_{2q} *and* R_{2q+2}. *Furthermore, if* z *is* 0 *for* $T = 0$ *then the same holds for all* z_j.

Proof. Let $f_i(V, Z) = \sum_{j=0}^{M} f_{ij}(V) Z^j$. The lemma will be proved by induction on the integer $\min._i \operatorname{order}_T f_i(v,z) - \min._{ij} \operatorname{order}_T[f_{ij}(v)z^j]$; the proof will be divided into two parts.

---

[3] In the following $k[[T]]$ is the power-series ring in a letter T over the field k.

A. Let $\min._i \operatorname{order}_T f_i(v,z) - \min._{ij} \operatorname{order}_T[f_{ij}(v)z^j] = 0$. In order to simplify notation, write $\lambda_j = \min._i \operatorname{order}_T f_{ij}(v)$ and $\mu_j = \min._i \operatorname{order}_T[f_{ij}(v)z^j]$. If $r = \operatorname{order}_T z$, then $\mu_j = \lambda_j + rj$. With the above assumption, we have $\min._j \mu_j = \min._i \operatorname{order}_T f_i(v,z)$. There is an index q $(0 \leqq q \leqq M)$ uniquely determined by the conditions

$$(1) \qquad \mu_q = \min._j \mu_j \text{ and } \mu_j > \mu_q \text{ for } j > q.$$

If $q = 0$, the sequence of elements mentioned in the conclusions of the lemma is obtained by taking $z_0 = z$, $z_1 = z$, $z_2 = 0$; then for the points R_j we have $R_0 = R_1 = R_2$. Next we will proceed by induction on the integer q.

Clearly, the proof of part **A.** will be completed if it is possible to construct elements z^* and z' of $k'[[T']]$, where T' is a fractional power of T and where $k' \supset k$ and:

a. Not all the $f_i(v,z^*)$ are 0 and not all the $f_i(v,z')$ are 0. If R, R^* and R' are the points obtained (as explained in the conclusions of the lemma) by substituting $T' = 0$ in the ratios of the $f_i(v,z)$, the $f_i(v,z^*)$ and the $f_i(v,z')$, then the locus of R^* over k is a rational curve and R and R' are points on this curve.

b. If $\mu'_j = \min._i \operatorname{order}_{T'}[f_{ij}(v)z'^j]$, then $\min._j \mu'_j = \min._i \operatorname{order}_{T'} f_i(v,z')$.

c. If q' is such that $\mu'_{q'} = \min._j \mu'_j$ and $\mu'_j > \mu'_{q'}$ for $j > q'$, then $q' < q$.

d. If $\operatorname{order}_T z$ is positive, then the orders in T' of z^* and z' are positive.

In order to construct elements z^* and z', consider the expressions[4] $(\lambda_j - \lambda_q)/(q-j)$ for $j < q$. There is a uniquely determined integer q' $(0 \leqq q' < q)$ such that

$$(2) \qquad \begin{cases} (\lambda_{q'} - \lambda_q)/(q-q') \text{ is the minimum of the expressions} \\ (\lambda_j - \lambda_q)/(q-j) \text{ for } j < q \text{ and } (\lambda_j - \lambda_q)/(q-j) > \\ (\lambda_{q'} - \lambda_q)/(q-q') \text{ for } j < q'. \end{cases}$$

---

[4] This expression arises in the following way: What should the order in T of z be, if we want, for a certain fixed $j<q$, $\min._i \operatorname{order}_T[f_{ij}(v)z^j] = \min._i \operatorname{order}_T[f_{iq}(v)z^q]$? The answer is $(\lambda_j - \lambda_q)/(q-j)$. Since $\mu_j = \lambda_j + rj$ and $\mu_q = \min._j \mu_j$, we have that $r \leqq \min._{j<q}(\lambda_j - \lambda_q)/(q-j)$. If now z^* is an element of $k[[T]]$ whose order (in T) is precisely this minimum, then there remains, for some i, a term $f_{iq}(v)z^{*q}$ among the terms of lowest order in T.

Let $T' = T^{1/(q-q')}$; if $\lambda'_j = \min._i \operatorname{order}_{T'} f_{ij}(v)$ then $\lambda'_j = \lambda_j(q - q')$, Suppose $z = \alpha_r T^r +$ higher powers in T $(\alpha_r \in k)$; take two independent transcendentals over k, β^* and β', write $k' = k(\beta^*, \beta')$ and let $z^* = \beta^* T^{(\lambda_{q'} - \lambda_q)/(q-q')}$, i.e.,. $z^* = \beta^* T'^{(\lambda_{q'} - \lambda_q)}$. If

$$\mu^*_j = \min._i \operatorname{order}_{T'} [f_{ij}(v) z^{*j}] \text{ then } \mu^*_j = \lambda_j(q - q') + j(\lambda_{q'} - \lambda_q).$$

By the assumptions, not all the λ_j are infinite, hence it follows that not all the μ^*_j are infinite. Since β^* is transcendental over k, it follows that not all the $f_i(v, z^*)$ are zero. Furthermore,

$$\begin{aligned} \mu^*_j - \mu^*_q &= (\lambda_j - \lambda_q)(q - q') + (j - q)(\lambda_{q'} - \lambda_q) \\ &= (\mu_j - \mu_q)(q - q') + (j - q)(\mu_{q'} - \mu_q). \end{aligned}$$

It follows from this by (1) and (2) that

$$(3) \qquad \mu^*_{q'} = \mu^*_q = \min._j \mu^*_j; \; \mu^*_j > \mu^*_{q'} \text{ for } j > q \text{ and for } j < q'.$$

Now let R^* and R be the above mentioned points (see **a**.). Since β^* is transcendental over k, it follows that the homogeneous coordinates of R^* are polynomials in β^* with coefficients in k. From the relations (1), (2) and (3) it follows that $R^* \to R$ over k (take $\beta^* \to \alpha_r$ if $\mu_q = \mu_{q'}$, and $\beta^* \to \infty$ if $\mu_q < \mu_{q'}$).

Next we will make the assumption that the index q' fulfills the condition

$$(4) \qquad q' < \min._{j<q'} (\mu^*_j - \mu^*_{q'}).$$

This assumption can be made; for by the inequalities of (3), this minimum is positive and it can then be made arbitrarily large by replacing T' by a power of T'. Now let $z' = \beta' T'^{(\lambda_{q'} - \lambda_q)+1}$; if $\mu'_j = \min._i \operatorname{order}_{T'} [f_{ij}(v) z'^j]$ then $\mu'_j = \mu^*_j + j$. From this, in combination with (3) and (4), it follows that

$$(5) \qquad \mu'_{q'} = \min._j \mu'_j; \; \mu'_j > \mu'_{q'} \text{ for } j > q' \text{ and } j < q'.$$

Since by construction $q' < q$, it follows that z' fulfills condition **c**. Again, since β' is transcendental over k, it follows that not all the $f_i(v, z')$ are zero; therefore, it is possible to construct a point R' by putting $T' = 0$ in the ratios of the $f_i(v, z')$. Further, since β' is transcendental over k, it also follows that $\mu'_{q'} = \min._j \mu'_j = \min._i \operatorname{order}_{T'} f_i(v, z')$; therefore, z' fulfills condition **b**. Next, we want to show that $R^* \to R'$ over k. It follows from the inequalities in (5) that R' is the point obtained by substituting $T' = 0$ in the ratios of the homogeneous coordinates of the point $[f_{0q'}(v), \cdots, f_{mq'}(v)]$. As we have seen above, the homogeneous coordinates of the point R^* are polynomials in β^* with coefficients in k; by (3) these polynomials begin with terms of degree q' in the β^* (and end with terms of degree q). Substituting $\beta^* = 0$ in the homogeneous coordinates of R^* therefore leads to the same point as substituting $T' = 0$ in the homogeneous coordinates of the point $[f_{0q'}(v), \cdots, f_{mq'}(v)]$, i.e., to the point R' as we have just seen. Therefore, $R^* \rightarrow R'$ over the specialization $\beta' \rightarrow 0$ with respect to k, and hence **a.** is satisfied by z^* and z'. It remains to be shown that **d.** is also fulfilled. As before, write $z = \alpha_r T^r + \cdots$. From the fact that $\mu_q \leqq \mu_{q'}$ (by (1)) and that $\mu_j = \lambda_j + jr$, it follows that $r \leqq (\lambda_{q'} - \lambda_q)/(q - q')$. Since $T = T'^{(q-q')}$, $z^* = \beta T'^{(\lambda_{q'}-\lambda_q)}$ and $z' = \beta' T'^{(\lambda_{q'}-\lambda_q)+1}$, it follows that

$$\text{order}_{T'} z \leqq \text{order}_{T'} z^* \leqq \text{order}_{T'} z'.$$

Hence **d.** is satisfied, which completes the proof of **A.**

B. Assume that the lemma is proved if the difference $\min._i \text{order}_T f_i(v, z) - \min._{ij} \text{order}_T [f_{ij}(v) z^j]$ is smaller then some integer d. Now suppose this difference is equal to d.

Let R and S be the points obtained by substituting $T = 0$ in the ratios of the $f_i(v, z)$ and the $f_i(v, 0)$, respectively. We adopt the following terminology during the rest of the proof of this lemma to simplify notation. If z and z' are elements of a ring $K[[T]]$ such that not all the $f_i(v, z)$ are 0 and not all the $f_i(v, z')$ are 0, and if R, respectively R', are the points obtained by substituting $T = 0$ in the ratios of the $f_i(v, z)$, respectively the $f_i(v, z')$, then we will call a sequence of points $R = R_0, R_1, \cdots, R_j, \cdots, R_{2n} = R'$ a *connecting sequence of points* between R and R' if the following are true: Every point R_j is obtained by means of an element z_j of $K[[T]]$ and a substitution $T = 0$ in the ratios of the $f_i(v, z_j)$ (which implies that not all the $f_i(v, z_j)$ are 0), and both R_{2q} and R_{2q+2} are specializations of R_{2q+1} over k for $q = 0, 1, \cdots, n-1$ (it is a tacit agreement that K contains k; it should be noted that in the present terminology—which is only used during the proof of this lemma—the field k plays a particular role). Further, if z and z' are 0 for $T = 0$ then we require the same for all the z_j. Moreover, we will call such a sequence $R = R_0, R_1, \cdots, R_{2n} = R'$ a *linearly connecting sequence of points* between R and R' if, for every triple $(2q, 2q+1, 2q+2)$ of this sequence, either $R_{2q} = R_{2q+1} = R_{2q+2}$ or there is a rational curve C_q having R_{2q+1} as a generic point over a suitable field containing k, and going through R_{2q} and R_{2q+2}.

Write $Z = X + Y$, let

$$f_i(V, Z) = \sum_{j=0}^{M} f_{ij}(V) Z^j = \sum_{j=0}^{M} g_{ij}(V, X) Y^j = g_i(V, X, Y).$$

(Note that $f_i(V,X)=g_{i0}(V,X)$.) Let $z=\alpha_r T^r+\alpha_{r+1}T^{r+1}+\alpha_{r+2}T^{r+2}+\cdots$, where $\alpha_r,\alpha_{r+1},\cdots\in k$. Let β be transcendental over k and take $x=\alpha_r T^r+\beta T^{r+1}$. Now, by the assumptions not all the $f_i(v,0)$ are zero, therefore, since β is transcendental over k, not all the $f_i(v,x)=g_{i0}(v,x)$ are zero. Let R_I be the point obtained by substituting $T=0$ in the ratios of the $f_i(v,x)$. Next let γ be transcendental over $k(\beta)$ and let $y=T^r(-\alpha_r+\gamma-\beta T)$, i.e., $x+y=\gamma T^r$. Since γ is transcendental over k, it follows that

$$(6)\qquad \min._i \operatorname{order}_T f_i(v,x+y)=\min._{ij}\operatorname{order}_T[f_{ij}(v)(x+y)^j].$$

The right hand side of (6) being finite implies that not all the $f_i(v,x+y)$ are 0, let R_{II} be the point obtained by substituting $T=0$ in the ratios of the $f_i(v,x+y)$. It follows by (6) and the special case of the lemma proved under **A.** that (in the just mentioned terminology) there is a linearly connecting sequence of points between R_{II} and S. We will show next that there is also a linearly connecting sequence of points between R_{II} and R_I. Consider the polynomials $g_i(V,X,Y)$ in the indeterminates $V_1,\cdots,V_h$, X and Y and consider the elements $v_1,\cdots,v_h$, x and y of $k(\beta,\gamma)[[T]]$. Since γ is transcendental over $k(\beta)$ it follows that

$$\min._i \operatorname{order}_T g_i(v,x,y)=\min._{ij}\operatorname{order}_T[g_{ij}(v,x)y^j].$$

R_{II} and R_I being the points obtained by substituting $T=0$ in the ratios of the $f_i(v,x+y)=g_i(v,x,y)$ and the $f_i(v,x)=g_i(v,x,0)$ respectively, it follows therefore by the special case of the lemma proved under **A.** that there is a linearly connecting sequence of points between R_{II} and R_I. (Note that if $\operatorname{order}_T z$ is positive then the orders in T of x, y and $x+y$ are positive, and therefore, by the special case of the lemma proved under **A.**, every intermediate point R_j is obtained by means of a z_j which has positive order in T.)

From the facts proved above, it follows that it is sufficient to prove that there is a linearly connecting sequence of points between R and R_I; the points R, respectively R_I, are obtained by putting $T=0$ in the $f_i(v,z)$, respectively the $f_i(v,x)=g_i(v,x,0)$. Now, let

$$y'=(\alpha_{r+1}-\beta)T^{r+1}+\alpha_{r+2}T^{r+2}+\cdots,\ \text{i.e.,}\ z=x+y';$$

then R can also be obtained by substituting $T=0$ in the $f_i(v,x+y')=g_i(v,x,y')$. If μ_q is the integer introduced in (1), i.e., $\min._{i,j}\operatorname{order}_T[f_{ij}(v)z^j]$, then it follows from the way in which the x and y' are chosen that the terms of degree μ_q in T have cancelled in the $g_i(v,x,y')$, and hence

$$\min._{ij}\operatorname{order}_T[f_{ij}(v)z^j]<\min._{ij}\operatorname{order}_T[g_{ij}(v,x)y'^j].$$

Since $f_i(v, z) = g_i(v, x, y')$, we then have that

$$\min._i \operatorname{order}_T g_i(v, x, y') - \min._{ij} \operatorname{order}_T [g_{ij}(v, x) y'^j]$$

is smaller than $\min._i \operatorname{order}_T f_i(v, z) - \min._{ij} \operatorname{order}_T [f_{ij}(v) z^j]$. We can now apply the induction hypothesis to the polynomials $g_i(V, X, Y)$ (instead of the $f_i(V, Z)$), to the elements $v_1, \cdots, v_h, x$ (instead of the $v_1, \cdots, v_h$) and y' (instead of the z) and to the points R and R_I obtained, respectively, by putting $T = 0$ in the ratios of the $g_j(v, x, y')$ and the $g_i(v, x, 0)$. This completes the proof of the lemma.

THEOREM 1. *Let W be a subvariety of $S^n \times P^m$ (n-space and projective m-space). Suppose the projection of W on S^n is equal to S^n itself, and let $[W: S^n] = 1$. Let Q be a point of S^n. Then $W\{Q\}$ is linearly connected.*

Proof. We will proceed by induction on the integer n; for $n = 1$ the theorem is clearly true.

Let k be a field of definition for W. Without loss of generality, it may be assumed that Q is the origin O of S^n and that k is algebraically closed, so that, in particular, the components of $W\{O\}$ are defined over k.

Let (x, y) be a generic point of W over k, where $(x) = (x_1, \cdots x_n)$ and where $(y) = (y_0, \cdots, y_m)$ are homogeneous coordinates in P^m, with $y_i = f_i(x)$, $f_i(X) \in k[X_1, \cdots, X_n]$. Write

(1) $f_i(X) = \sum_{j=s}^{t} f_{ij}(X)$ with $f_{ij}(X)$ homogeneous of degree j and for at least one i, $f_{is}(X)$ is different from zero.

First we will fix, in a certain way, a point R_0 in $W\{O\}$, and then we show that every point in $W\{O\}$ is linearly connected in $W\{O\}$ with this point R_0. We fix this point R_0 as follows. Let the quantities u_i be defined by the equations

$$x_i = u_i x_1, \qquad i = 2, 3, \cdots, n. \tag{2}$$

Let $(x, u) \rightarrow (0, u')$ over k, with u'_i independent transcendentals over k. There exists an index j_0 such that $f_{j_0 s}(X) \neq 0$, the quotients y_j / y_{j_0} then have a unique specialization over the specialization $(x, u) \rightarrow (0, u')$ with reference to k; this specialization determines a point R_0 in $W\{O\}$. We note that R_0 depends only on the $f_{is}(X)$ and on the specialization of the ratios of the x_i, and not on the particular index 1 chosen to define the quantities u_i.

Now suppose there is given a point R in $W\{O\}$, we will show that R is linearly connected with R_0 in $W\{O\}$. Let $k(R)$ be the field obtained from adjoining to k the non-homogeneous coordinates of R. It is possible to construct a field K, containing $k(R)$, and a homomorphism $\phi: k[x] \rightarrow K[[T]]$, leaving k invariant, such that the point R can be obtained from substituting $T=0$ in the ratios of the $\phi[f_i(x)]$ (this implies, in particular, that not all the $\phi[f_i(x)]$ are 0); moreover, this ϕ can be constructed in such a way that not all the $\phi[f_{is}(x)]$ are 0. (The construction of such a field K and homomorphism ϕ can be done in the following way. Take a linear space L^{m+1} generic through the point $O \times R$, then $W \cap L$ consists of curves C_i [see, for instance, the proof of Prop. 7 of App. II of [I]]; let C_1 go through the point $O \times R$. Let K be the algebraic closure of the field which is obtained from adjoining to $k(R)$ the coefficients of a set of equations of L. A generic point (x) of C_1 over K is a generic point of W over k [see again [I], App. II, proof of Prop. 7]. Take a valuation on C_1 with center $O \times R$, this determines a homomorphism of $K[x] \rightarrow K[[T]]$; the restriction to $k[x]$ fulfills all the requirements.)

Given the point R, we construct such a field K and homomorphism $\phi: k[x] \rightarrow K[[T]]$. Among the $x_1, \cdots, x_n$, for instance x_1 starts with a term of lowest degree in T. Introducing the u_i as in (2), ϕ can now be extended to $k[u, x_1] \rightarrow K[[T]]$. Let the extension still be denoted by ϕ. To distinguish x_1 from the other x_i write $x_1 = z$, then we have

$$x_1 = z, \qquad x_i = u_i z; \qquad i = 2, 3, \cdots, n. \tag{3}$$

Note that z is transcendental over $k(u)$; therefore, the specialization of z over every specialization of the $u_2, u_3, \cdots, u_n$ with respect to k may be changed arbitrarily.

Now apply the lemma to the polynomials $\sum_{j=s}^{t} f_{ij}(U) Z^{j-s}$ (s was introduced in (1)) in the indeterminates $U_2, \cdots, U_n$ and Z with coefficients in the field K (which is analogous to the field k in the lemma), and to the elements $\phi(u_2), \cdots, \phi(u_n)$ and $\phi(z)$ in the ring $K[[T]]$. The homomorphism ϕ was constructed in such a way that not all the $\phi[f_{is}(u)] = f_{is}[\phi(u)]$ are 0, R was the point obtained by putting $T=0$ in the ratios of the $f_i[\phi(x)]$, i.e., in the ratios of the $\sum_{j=s}^{t} f_{ij}[\phi(u)]\phi(z)^{j-s}$; let S be the point obtained by putting $T=0$ in the ratios of the $\phi[f_{is}(u)]$. By the lemma, there is a sequence of points $R = R_0, R_1, \cdots, R_{2p} = S$, such that, for every triple $(2q, 2q+1, 2q+2)$, either $R_{2q} = R_{2q+1} = R_{2q+2}$ or there is a rational curve C_q, going through R_{2q} and R_{2q+2}, and having R_{2q+1} as a generic point over some field containing K (and hence, a fortiori containing k, over which the components of $W\{O\}$ are defined). Moreover, since $\phi(z)=0$ for $T=0$, it follows by the last conclusion of the lemma and by the relations (3) that all the points R_j are in $W\{O\}$. Therefore, the sequence of points between R and S is a linearly connecting sequence of points in $W\{O\}$.

R_0 being constructed as in the beginning of the proof by means of a generic specialization of the ratios of the x_i, both R_0 and S are specializations over k of the point T with homogeneous coordinates $[f_{0s}(x),\cdots,f_{ms}(x)]$ in P^m, where $f_{is}(X)$ is homogeneous of degree s (see (1)). Let X be the locus of R_0 over k. Since R_0 is constructed by means of a generic specialization of the ratios of the x_i, it follows that X is also the locus of the point T over k; in particular $S\in X$. Since the components of $W\{O\}$ are defined over k (which is algebraically closed), it follows that X is in a component of $W\{O\}$. In order to complete the proof, it suffices to show that S and R_0 are linearly connected in X. Consider the locus Y over k of the point with coordinates $[x_1,\cdots,x_n;\ f_{0s}(x),\cdots,f_{ms}(x)]$ where the $(x_1,\cdots,x_n)$ are considered as homogeneous coordinates in P^{n-1} and, as before, $[f_{0s}(x),\cdots,f_{ms}(x)]$ are homogeneous coordinates in P^m. Then the variety Y in $P^{n-1}\times P^m$ is a birational transformation of P^{n-1}; hence, by our induction hypothesis (see beginning of the proof), the total transform by Y of every point of P^{n-1} is linearly connected. By this, the projection of Y on P^m is linearly connected; however, this projection is X. This completes the proof.

2. Multiplicities of maximal connected bunches in specializations of complete sets of conjugates. Let U and V be varieties and let W be a subvariety of $U\times V$. Suppose the projection of W on U is equal to U itself and let $\dim. W=\dim. U$. Let k be a field of definition for U, V and W and let Q be a generic point of U over k. It follows easily from [I], Chap. IV, Th. 6, that every point of $W\cap(Q\times V)$ is generic on W over k and the points of this intersection are conjugates of each other over $k(Q)$. Further, all the different conjugates over $k(Q)$ occur among the points of this intersection.

THEOREM 2. *Let W be a subvariety of $S^n\times P^m$ (n-space and projective m-space), let* $\dim. W=n$ *and suppose the projection of W on S^n is equal to S^n itself. Let k be a field of definition for W and let $Q\times R$ be a generic point of W over k. Let $(R^{(1)},\cdots,R^{(g)})$ be a complete set of conjugates of R over $k(Q)$. Suppose Q' is a point of S^n and let $\mathfrak{B}$ be a maximal connected bunch of $W\{Q'\}$. Then, in every specialization of $(R^{(1)},\cdots,R^{(g)})$ over the specialization $Q\to Q'$ with reference to k, the* *multiplicity of the bunch* $\mathfrak{B}$ *is the same. (The multiplicity of* $\mathfrak{B}$ *in a specialization* $(R'^{(1)},\cdots,R'^{(g)})$ *of* $(R^{(1)},\cdots,R^{(g)})$ *over the specialization* $Q\rightarrow Q'$ *with reference to* k *is defined as the number of points* $R'^{(\eta)}$ *which are in* $\{\mathfrak{B}\}$.) *Further, if* $\mathfrak{B}$ *occurs with multiplicity* 1, *then* $\mathfrak{B}$ *is linearly connected.*

Proof. On W, consider the cycle $\sum_{\eta=1}^{g} Q\times R^{(\eta)}$ and let T be its Chow-point. The ratios of the coordinates of T are in $k(Q)$. Let Z be the locus of (Q,T) over k; Z fulfills the conditions of Theorem 1. Hence $Z\{Q'\}$ is linearly connected. Let $(Q',R'^{(1)},\cdots,R'^{(g)})$ and $(Q',R''^{(1)},\cdots,R''^{(g)})$ be two specializations of $(Q,R^{(1)},\cdots,R^{(g)})$ over k and let T' and T'' be the Chow-points of $\sum_{\eta=1}^{g} Q'\times R'^{(\eta)}$ and $\sum_{\eta=1}^{g} Q'\times R''^{(\eta)}$ respectively. Let K be the algebraic closure of the field $k(Q')$; the components of $Z\{Q'\}$ and $W\{Q'\}$ are defined over K. T' and T'' are points in $Z\{Q'\}$; since $Z\{Q'\}$ is connected, it follows that there is a sequence of points T'_j $(j=0,1,\cdots,2p;\ T'_0=T',\ T'_{2p}=T'')$ in the components of $Z\{Q'\}$ such that T'_{2i} and T'_{2i+2} are both specializations of T'_{2i+1} over K for $i=0,1,\cdots,p-1$. Let $(R'_j{}^{(1)},\cdots,R'_j{}^{(g)})$ be a specialization of $(R^{(1)},\cdots,R^{(g)})$ over the specialization $(Q,T)\rightarrow(Q',T'_j)$, with reference to k, for $j=0,1,\cdots,2p$. Since, by the properties of Chow-points, the cycle $\sum_{\eta=1}^{g} Q'\times R'_j{}^{(\eta)}$ is uniquely determined by the point T'_j, it follows that, for a suitable order of the points $R'_{2i}{}^{(\eta)}$, the set $(T'_{2i},R'_{2i}{}^{(1)},\cdots,R'_{2i}{}^{(g)})$ is a specialization of $(T'_{2i+1},R'_{2i+1}{}^{(1)},\cdots,R'_{2i+1}{}^{(g)})$ over K, and similarly for $2i+2$ (where $i=0,1,\cdots,p-1$). The components of $W\{Q'\}$ being defined over K, this completes the first part of the proof.

Assume now that $\mathfrak{B}$ has multiplicity 1 and let, for every j, $R'_j{}^{(1)}$ be the unique point in $\{\mathfrak{B}\}$. Under the present assumptions we have then $K(R'_j{}^{(1)})\subset K(T'_j)$. The linear connectedness of $\mathfrak{B}$ then follows from the linear connectedness of $Z\{Q'\}$.

Note. Theorem 2 is a generalization of [I], Chap. III, Th. 4, except that, if $\{\mathfrak{B}\}$ reduces to a point R' (i.e., R' is a proper specialization of R over the specialization $Q\rightarrow Q'$ with reference to k), then the multiplicity of R' is a multiple of $[k(Q',R'):k(Q')]_i$. However this result can also be obtained from Theorem 2 and the theory of algebraic functions of one variable. We sketch a proof.[5] By an extension of the ground field and a change of coordinates it can be assumed that $Q'=0$. Write $Q=(x_1,\cdots,x_n)$,

---

[5] Cf. [I], Chapter III, Theorem 2 and G. Shimura, *American Journal of Mathematics*, vol. 77 (1955), page 141, Prop. 13.

$R=(1,y_1,\cdots,y_m)$ $x_1=\lambda$ and $u_i=x_i/\lambda$ for $i=2,3,\cdots,n$. Consider the specialization $(x,u)\rightarrow(0,u)$ over k and let $K=k(u)$. Next consider (y) as functions of one variable λ over K. Let Ω be the completion of $K(\lambda)$ with respect to the valuation induced in $K(\lambda)$ by $\lambda\rightarrow 0$. It follows by Theorem 2 that there is a conjugate $R^{(\eta)}$ of R over $k(x)$, such that R' is a specialization of $R^{(\eta)}$ over the valuation induced by $\lambda\rightarrow 0$ in Ω. The required result then follows essentially from the fact that every specialization of $R^{(\eta)}$ over the valuation induced by $\lambda\rightarrow 0$ in Ω, is a conjugate of R' over K (since Ω is complete) and from the fact that $[K(R'):K]$ is a factor of $[\Omega(R^{(\eta)}):\Omega]$.

The following proposition is a generalization of [I], Chap. III, Prop. 9 and can be proved by the same methods.

PROPOSITION 1. *Let W be a subvariety of $S^n\times P^m$, snch that* dim. $W=n$, *and let the projection of W on S^n be equal to S^n itself. Let k be a field of definition for W. Let τ be an isomorphism of k and a field k'. Suppose Q and Q' are points of S^n such that τ can be extended to an isomorphism of $k(Q)$ and $k'(Q')$; let π be an extension of τ to the algebraic closures of $k(Q)$ and $k'(Q')$. Let $\mathfrak{B}$ be a maximal connected bunch of $W\{Q\}$. Then $\mathfrak{B}^\pi$ is a maximal connected bunch of $W^\tau\{Q'\}$. Let (x,y) and (x',y') be generic points of W and W^τ over k and k' respectively, then the multiplicities of $\mathfrak{B}$ and $\mathfrak{B}^\pi$ in the specializations of a complete set of conjugates of (y) over $k(x)$, respectively (y') over $k'(x')$, over the specialization $(x)\rightarrow Q$ with respect to k, respectively $(x')\rightarrow Q'$ with respect to k', are equal.*

THEOREM 3.[6] *Let W be a subvariety of $U\times V$, where V is a projective variety. Let* dim. $W=$ dim. U *and let the projection of W on U be equal to U. Let k be a field of definition for U, V and W and let (Q,R) be a generic point of W over k (hence Q is generic on U over k). Suppose Q' is a simple point on U and let $\mathfrak{B}$ be a maximal connected bunch of $W\{Q'\}$. Let $(R^{(1)},\cdots,R^{(g)})$ be a complete set of conjugates of R over $k(Q)$. Then, for every specialization $(R'^{(1)},\cdots,R'^{(g)})$ of $(R^{(1)},\cdots,R^{(g)})$ over the specialization $Q\rightarrow Q'$ with respect to k, the number of points $R'^{(\eta)}$ which are in $\{\mathfrak{B}\}$ is the same. Further, if $\mathfrak{B}$ is represented only once in such a specialization, then $\mathfrak{B}$ is linearly connected.*

Proof. Suppose U^n is a variety in S^N (eventually P^N) and V^m is a variety in P^M. Let $F_i(X)$, $i=1,2,\cdots,n$, be a uniformizing set of linear forms for U at Q' with coefficients in k; by [I], Chap. IV, Prop. 25, this is a fortiori a uniformizing set of linear forms for U at Q. Write $Q=(x)$ and

---

[6] Theorem 3 is the analogue of [I], Chap. VI, Th. 12.

$Q' = (x')$; let L and L' be the linear varieties in S^N defined, respectively, by the equations $F_i(X-x)=0$ and $F_i(X-x')=0$, $i=1,\cdots,n$. These equations can also be written in the form $F_i(X)-v_i=0$ and $F_i(X)-v'_i=0$ with $v_i=F_i(x)$ and $v'_i=F_i(x')$ respectively. By [I], Chap. V, Prop. 20, Q and Q' are proper components of $U\cap L$, respectively of $U\cap L'$, and of multiplicity 1. By [I], Chap. IV, Prop. 24 $k(Q)$ is algebraic (and separable) over $k(v)$. From the fact that Q' is a proper component of $U\cap L'$ of multplicity 1, it follows by [I], Chap. V, Cor. 1 of Th. 3 that Q' is a proper specialization of Q, over the specialization $(v)\rightarrow(v')$ with reference to k, of multiplicity 1. Let $(Q^{(1)},\cdots,Q^{(d)})$ be a complete set of conjugates of Q over $k(v)$ and let $Q^{(1)}=Q$. A complete set of conjugates of (Q,R) over $k(v)$ consists of the dg points $(Q^{(\tau)},R^{(\tau\eta)})$, $\tau=1,\cdots,g$, where the set of points $(R^{(\tau 1)},\cdots,R^{(\tau g)})$ is obtained from $(R^{(1)},\cdots,R^{(g)})$ by applying to the algebraic closure of $k(v)$ an automorphism over $k(v)$ such that Q is transformed in $Q^{(\tau)}$. Consider the locus X over k of the point (v,Q,R). X is a subvariety of $S^n\times P^N\times P^M$ (after, perhaps, a projective closure of S^N); since a product of projective spaces can be embedded in an everywhere biregular way into a projective space, it follows that X fulfills the conditions of Theorem 2.

Now let a specialization $(R'^{(1)},\cdots,R'^{(g)})$ of $(R^{(1)},\cdots,R^{(g)})$ over the specialization $Q\rightarrow Q'$ with reference to k be given; over this specialization (v) specializes necessarily to (v'). Next, extend this specialization to a specialization of all the $(Q^{(\tau)},R^{(\tau\eta)})$ over the specialization $(v)\rightarrow(v')$ with reference to k. If $\mathscr{B}$ is a maximal connected bunch of $X\{v'\}$; then by Theorem 2 the number of points $(Q'^{(\tau)},R'^{(\tau\eta)})$ which are in $\{\mathscr{B}\}$ is always the same, independently of the way in which the specialization $(v)\rightarrow(v')$ with reference to k is extended. Clearly, among the bunches $\mathscr{B}$ of $X\{v'\}$ there must be one which contains (as point set) $Q'\times\{\mathfrak{B}\}$; however, since Q' is a proper specialization of Q, over $(v)\rightarrow(v')$ with reference to k, it follows that $Q'\times\{\mathfrak{B}\}$ itself is such a bunch $\{\mathscr{B}\}$ (i.e., a maximal connected bunch of $X\{v'\}$). Now let $(Q'^{(\tau)},R'^{(\tau\eta)})$ be in $Q'\times\{\mathfrak{B}\}$; since Q' is a proper specialization of Q, over $(v)\rightarrow(v')$ with reference to k, of multiplicity 1, it follows that $\tau=1$, and hence also $R'^{(\tau\eta)}=R'^{(\eta)}$. As we have already seen above, the number of points $(Q'^{(\tau)},R'^{(\tau\eta)})$ which are in $Q'\times\{\mathfrak{B}\}$ is independent of the way in which the specialization $(v)\rightarrow(v')$, with reference to k, is extended; this implies, in particular, that the number of points $R'^{(\eta)}$ which are in $\{\mathfrak{B}\}$ is for all the specializations of $(R^{(1)},\cdots,R^{(g)})$ over $Q\rightarrow Q'$, with reference to k, the same. This completes the first part of the proof.

Next assume that there is only one point $R'^{(\eta)}$ in $\{\mathfrak{B}\}$. Then by what is proved above, it follows that there is only one point among the $(Q'^{(\tau)}, R'^{(\tau\eta)})$ which is in $Q' \times \{\mathfrak{B}\}$. Hence, by Theorem 2, $Q' \times \mathfrak{B}$ is linearly connected, and hence $\mathfrak{B}$ is linearly connected.

A direct consequence is the connectedness theorem mentioned in the introduction.

COROLLARY. *Let W be a subvariety of $U \times V$, where V is a projective variety. Suppose the projection of W on U is equal to U and let $[W:U] = 1$. Let Q' be simple on U. Then $W\{Q'\}$ is linearly connected.*

Note. This result is proved, except for the linearity, in [IV].

UNIVERSITY OF LEYDEN,
LEYDEN, THE NETHERLANDS.

REFERENCES.

[I] A. Weil, *Foundations of algebraic geometry*, Colloquium Publications, New York, 1946.

[II] ———, "Sur les critères d'équivalence en géométrie algébrique," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[III] O. Zariski, "Theory and applications of holomorphic functions on algebraic varieties over arbitrary groundfields," *Memoirs of the American Mathematical Society*, No. 5, 1951.

[IV] ———, *The connectedness theorem for birational transformations*, Princeton Series, No. 12 (A symposium in Honor of S. Lefschetz), 1957.

UNIQUENESS IN THE CAUCHY PROBLEM FOR PARTIAL DIFFERENTIAL EQUATIONS.*[1]

By A. P. Calderón.

1. Introduction. We begin with a few historical remarks. The classical theorem of Cauchy-Kowalewski asserts the existence of analytic solutions of analytic equations or systems of equations with analytic Cauchy data and their uniqueness in the class of analytic functions. In 1901 Holmgren [6] proved that the Cauchy problem has at most one continuous solution with continuous derivatives up to the order of the equations, provided that the latter are linear and have analytic coefficients. The condition on the coefficients is essential in Holmgren's argument and precludes the possibility of generalizing the result to the non-linear case. The first contribution in the direction of removing the assumption of analyticity was made in 1939 by T. Carleman [2], who proved the corresponding result in the case of two independent variables assuming that the characteristics of the equations are non-multiple. In view of the example of E. de Giorgi [3] (see also A. Plis [10]), who exhibited an example with multiple characteristics for which the Cauchy problem has more than one solution, the condition on the characteristics in Carleman's result no longer seems artificial, but, unfortunately, the restriction to two variables is indispensable to the method of proof. In the case of more than two variables, no essential progress was made until 1954 when C. Müller [8] studied a special second order equation. Later P. Hartman and A. Wintner [4] and E. Heinz [5] settled the case of quasilinear second order equations with the Laplacian as principal part. (See also P. D. Lax [7]). Shortly thereafter, N. Aronszajn [1] extended this result to general second order elliptic case. For other results on quasilinear equations with principal parts with constant coefficients, see also L. Nirenberg [9]. In the present paper, we shall generalize Carleman's theorem to functions of any number of variables with two exceptions, the case of three variables for equations and three or four variables for systems. The presence of these

---

* Received June 30, 1957.

[1] This research was partly supported by the United States Air Force under Contract No. AF18(600)-685 monitored by the Office of Scientific Research. The author is indebted to P. Olum and G. A. Hunt for help with this paper.

exceptional cases is due to topological difficulties in our approach. Whether they are really exceptional or not, we do not know. Since the non-multiplicity of the characteristics plays an essential role in our argument and it does not seem to be possible to introduce additional independent variables in a differential problem without sometimes causing multiplicities to appear in the characteristics, we have been unable to reduce the exceptional cases to the other. In special instances, though, such as that of second and third order equations, our result holds for any number of variables.

Our method is based on a representation of linear differential operators by means of singular integral operators. More specifically, if Au is a linear differential operator of homogeneous order m defined on all Euclidean space and with bounded coefficients, then $Au = H\Lambda^m u$, where Λ is a square root of the negative of the Laplacian and H is a singular integral operator. For operators such as H, there is an approximate functional calculus which allows us to reduce the problem of uniqueness to a simple form. The first section of the paper will be devoted to discussing the operators H and the representation of A briefly described above. For the proof of the basic properties, we shall refer the reader to a paper by A. Zygmund and the author (see [11]).

2. Singular integral operators. We begin this section with an informal discussion. Consider the real k-dimensional Euclidean space E_k, complex valued functions $u(x)$ on E_k, and the operator

$$H(u) = a(x)u(x) + \int_{E_k} h(x, x-z)u(z)\,dz, \tag{1}$$

where $a(x)$ is complex, bounded and $h(x,z)$ is complex homogeneous of degree $-k$ with respect to z, that is, $h(x,\lambda z) = \lambda^{-k}h(x,z)$ for $\lambda > 0$, where λz is the point with coordinates $\lambda z_1, \lambda z_2, \cdots, \lambda z_k$, and $z = (z_1, \cdots, z_k)$, and $h(x,z)$ has mean value zero on the sphere $S_{k-1} = \{|z| = (z_1^2 + \cdots + z_k^2)^{\frac{1}{2}} = 1\}$ for each x. Under mild assumptions on $h(x,z)$, the integral above is meaningful as a principal value integral for $u(x)$, say, square integrable over E_k. If $a(x)$ and $h(x,z)$ are actually independent of x, then Hu can be easily computed by taking Fourier transforms. Specifically, if $\hat{u}(x)$ denotes the Fourier transform of $u(x)$,[1a] then

$$\widehat{Hu} = (a + \hat{h})\hat{u}, \tag{2}$$

[1a] In contrast with [11] we use here the Fourier integral with a minus sign in the exponent. This accounts for apparent discrepancies in sign.

where $\hat{h}$ is the Fourier transform of $h(x,z) = h(z)$, the Fourier integral being taken as a principal value integral. If $h(z)$ is continuous in $|z| > 0$, then $\hat{h}(z)$ exists, is a homogeneous function of degree zero, that is, such that $\hat{h}(\lambda z) = \hat{h}(z)$ for every $\lambda > 0$, and has mean value zero on $S_{k-1} = \{|z| = 1\}$. Conversely, every sufficiently smooth function with these properties is the Fourier transform of some $h(z)$. The function $(a + \hat{h})$ in (2) is called the symbol of the operator H and we shall denote it by $\sigma(H)$. It is clear from (2) that operators with a and h independent of x can be multiplied and added by simply multiplying and adding their symbols.

Let now Au be a linear partial differential operator with constant coefficients of homogeneous order m. Then

$$\widehat{Au} = p_A(x) i^m \hat{u}(x), \tag{3}$$

where $p_A(x)$ is the characteristic form of the operator A. Let us rewrite the last identity as

$$\widehat{Au} = [p_A(x) \,|\, x \,|^{-m} i^m] \,|\, x \,|^m \, \hat{u}(x) \tag{4}$$

and define the operator Λ by

$$\widehat{\Lambda u} = |\, x \,|\, \hat{u}(x). \tag{5}$$

Then since the expression in square brackets in (4) is a homogeneous function of degree zero, it is the symbol of some singular integral operator H, and we obtain

$$\widehat{Au} = \sigma(H) \,|\, x \,|^m \hat{u}(x) = \sigma(H) \, (\Lambda^m u)^\wedge$$

and

$$Au = H \Lambda^m u, \tag{6}$$

where the symbol $\sigma(H)$ of H is given by $p_A(x) \,|\, x \,|^{-m} i^m$, $p_A(x)$ being the characteristic form of A. If A is the Laplacian, then

$$Au = \Delta u = - \Lambda^2 u,$$

which justifies the assertion that Λ is a square root of the negative of the Laplacian.

Suppose now that the coefficients of A are variable, that is,

$$Au = \sum_\alpha a_\alpha(x) D_\alpha u, \tag{7}$$

where $D_\alpha u$ runs over all partial derivatives of u of order m. Let us now represent each $D_\alpha u$ as in (16)

$$D_\alpha u = H_\alpha \Lambda^m u, \tag{8}$$

and substituting in (7), we obtain

$$(9) \qquad Au = \sum_{\alpha} a_\alpha(x) H_\alpha \Lambda^m u = (\sum a_\alpha H_\alpha) \Lambda^m u = H\Lambda^m u,$$

where $Hu = \sum a_\alpha H_\alpha u = \sum a_\alpha(x)(H_\alpha u)$. Now as is easily seen, since H_α is of the form (1), so are $a_\alpha H_\alpha$ and $H = \sum a_\alpha H_\alpha$. Thus we have obtained the desired representation of A in the case of variable coefficients.

Let us revert to the operators of the form (1). In the general case, that is, when a and h actually depend on x, we shall define the symbol $\sigma(H)$ of the operator H by

$$\sigma(H) = a(x) + \hat{h}(x, z),$$

where $\hat{h}(x,z)$ is the Fourier transform of $h(x,z)$ with respect to z. The symbol is now a function of two arguments, $x, z \in E_k$, which is homogeneous of degree zero with respect to z. One verifies that the symbol of the operator H in (9) is precisely $\sum a_\alpha(x) z^\alpha |z|^{-m} i^m$, where $z^\alpha = z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_k^{\alpha_k}$, and $\sum a_\alpha(x) z^\alpha$ is the characteristic form of the operator A.

The operators of the form (1) do not form an algebra under ordinary composition but it is possible to introduce a product $H_1 \circ H_2$ by means of the formula $\sigma(H_1 \circ H_2) = \sigma(H_1)\sigma(H_2)$. Under mild restrictions on the operators H, this product is always defined, and with this multiplication the class of singular integral operators becomes a commutative algebra which is isomorphic to the function algebra of their symbols. The interest of this kind of multiplication lies in the fact that it is a fairly satisfactory substitute for ordinary composition of operators which, incidentally, is non-commutative. More specifically, the difference between $H_1 \circ H_2$ and $H_1 H_2$ has the following property. Our operators H are bounded on $L^2(E_k)$ and Λ is densely defined in $L^2(E_k)$ and unbounded, but $H_1 \circ H_2 - H_1 H_2$ multiplied on the right or the left by Λ is bounded. Thus, modulo operators with the property of remaining bounded after multiplication by Λ, ordinary composition is equivalent to the formally simpler multiplication introduced above.

We now proceed to formulate precisely the properties of singular integral operators which we shall need. For their proof we refer the reader to [11].[1a] By C_β, $1 \leqq \beta \leqq 2$, we shall mean the class of bounded complex valued functions in C_1 with bounded first order derivatives satisfying a uniform Hölder condition of order $\beta - 1$. If $0 \leqq \beta < 1$, then C_β will stand for the class of bounded continuous functions satisfying a uniform Hölder condition of order β. By $C_\beta{}^\infty$, we shall mean the class of functions depending on two or more arguments which are in C^∞ with respect to the last argument and whose derivatives of all orders with respect to the coordinates of this are in C_β with respect to all variables. By L^2, we shall mean the class of functions on E_k with integrable square, and L_1^2 will stand for the class of functions in L^2 with first order derivatives (in the sense of Schwartz) in L^2. We shall say that the operator (1) is of type C_β^∞ if $a(x) \in C_\beta$ and $h(x,z) \in C_\beta^\infty$ in $|z| \geqq 1$. The letter c will stand for a constant not necessarily the same in each occurrence.

THEOREM 1. *Let $\beta \geqq 0$ be given. Consider the class of singular integral operators H of type C_β^∞. Then Hu is well defined as a principal value integral for $u \in L^2$ and Hu is in L^2. Further, H is a bounded operator on L^2. There exists a one-to-one linear mapping σ of the class of operators of type C_β^∞ onto the class of functions $F(x,z)$, $x, z \in E_k$ homogeneous of degree zero with respect to z and in C_β^∞ in $|z| \geqq 1$, such that, if N_H is the least upper bound for the absolute value of $F(x,z) = \sigma(H)$ (see footnote 2) and its derivatives with respect to coordinates of z of order $2k$ evaluated in $|z| \geqq 1$, then*

$$\|H\| \leqq cN_H, \tag{10}$$

where $\|H\|$ is the norm of H as an operator on L^2 and c is a constant depending only on k.

THEOREM 2. *If $u(x) \in L_1^2$ and $\hat{u}(x)$ denotes the Fourier transform of $u(x)$, then $\hat{u}(x)|x|$ belongs to L^2. Thus the operator Λ defined by $\widehat{\Lambda u} = \hat{u}(x)|x|$ has domain L_1^2, range in L^2 (see footnote 3) and is symmetric.*

THEOREM 3. *Let H be a singular integral operator of type C_β^∞ with $1 < \beta \leqq 2$. Let M_H denote the least upper bound for the absolute values of $\sigma(H) = F(x,z)$, its derivatives with respect to coordinates of z of order $2k$, the first order derivatives of these and of $F(x,z)$ with respect to coordinates of x, and the Hölder constants of the latter in $|z| \geqq 1$. Let H^* denote the adjoint of H and let $H^\#$, $H_1 \circ H_2$ be defined by*

$$\sigma(H^\#) = \bar{\sigma}(H), \qquad \sigma(H_1 \circ H_2) = \sigma(H_1)\sigma(H_2). \tag{11}$$

Then $H^\#$ and $H_1 \circ H_2$ are singular integral operators of type C_β^∞. Further, if H is of type C_β^∞ and $u \in L_1^2$, then Hu and H^*u are in L_1^2, so that the operators ΛH, $H\Lambda$, $H^*\Lambda$, ΛH^* are defined on L_1^2. Further, if $u \in L_1^2$, then

---

[2] The function $\sigma(H)$ here is the symbol of H.

[3] The definition of the operator Λ given here is different from the one given in [11]. They are, nevertheless, readily seen to be equivalent.

$$\begin{aligned} &\|(\Lambda H - H\Lambda)u\| \leqq cM_H \|u\|, \qquad \|\Lambda(H^* - H^\#)u\| \leqq cM_H \|u\|, \\ &\qquad\qquad \|(H^* - H^\#)\Lambda u\| \leqq cM_H \|u\|, \\ &\|\Lambda(H_1 \circ H_2 - H_1H_2)u\| \leqq cM_{H_1}M_{H_2} \|u\|, \\ &\qquad\qquad\qquad \|(H_1 \circ H_2 - H_1H_2)\Lambda u\| \leqq cM_{H_1}M_{H_2} \|u\|, \end{aligned} \tag{12}$$

where c is a constant depending on k only and the norms are L^2-norms. Consequently, the operators in (12) *can be extended continuously to bounded operators on L^2.*

THEOREM 4. *If H_1 and H_2 are in C_β^∞, $\beta \geqq 0$ and the functions $\sigma(H_1) = F_1(x, z)$, $\sigma(H_2) = F_2(x, z)$ are independent of x, then $H_1 \circ H_2 = H_1H_2$, $H_1^\# = H_1^*$ and H_1 has an inverse if and only if $\sigma(H_1)$ does not vanish. Further, H_1 takes L_1^2 into L_1^2 and $H_1\Lambda = \Lambda H_1$.*

THEOREM 5. *Let $A = \sum_\alpha a_\alpha(x)D_\alpha$, where $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_k)$, $\alpha_1 + \alpha_2 + \cdots + \alpha_k = m$, and $D_\alpha = \partial^{\alpha_1+\alpha_2+\cdots+\alpha_k}/\partial x_1^{\alpha_1}\partial x_2^{\alpha_2}\cdots\partial x_k^{\alpha_k}$ be a linear homogeneous differential operator of homogeneous order m with coefficients $a_\alpha(x)$ in C_β, $\beta \geqq 0$. If $u(x)$ is in L^2 and has derivatives of orders less than or equal to m in L^2, then $\Lambda^m u$ is defined and $Au = H\Lambda^m u$, where H is a singular integral operator of type C_β^∞ and*

$$\sigma(H) = i^m \sum a_\alpha(x) z^\alpha |z|^{-m}, \tag{13}$$

where $z^\alpha = z_1^{\alpha_1}z_2^{\alpha_2}\cdots z_k^{\alpha_k}$. In particular, if $u \in L_1^2$, then

$$\partial u/\partial x_j = iR_j\Lambda u = i\Lambda R_j u, \tag{14}$$

where $\sigma(R_j) = z_j|z|^{-1}$. Conversely, if $u \in L_1^2$, then

$$i\Lambda u = \sum_{j=1}^{k} R_j \partial u/\partial x_j = \sum_{j=1}^{k} \partial R_j u/\partial x_j. \tag{15}$$

In what follows, we shall consider singular integral operators depending on a parameter t and function $u(t)$ depending on t and with values in L^2. We shall say that such a function is continuous if $\|u(t) - u(t_0)\|$ tends to zero as t tends to t_0 for all t_0. We shall say that $u(t)$ is differentiable if there exists a function $du/dt = v(t)$ of the same type such that

$$\|(u(t) - u(t_0))/(t - t_0) - v(t_0)\|$$

tends to zero as t tends to t_0, for all t_0.

Our results on uniqueness are essentially applications of the following

LEMMA 1. *Let $u(t)$, $0 \leqq t \leqq h$, have values in L_1^2, be continuously*

P14918

differentiable and be such that $\Lambda u(t)$ is continuous. Let $P(t)$ and $Q(t)$ be singular integral operators such that $\sigma(P) = F_1(t,x,z)$ and $\sigma(Q) = F_2(t,x,z)$ are real and in C_β^∞, $\beta > 1$ in $|z| \geqq 1$.[4] *Assume that $P(t)$ has a two sided inverse for each t or else vanishes identically, and let $\phi_n(t) = (t + 1/n)^{-n}$. Then if $u(0) = 0$ and*

$$\int_0^h \phi_n^2 \| du/dt + (P + iQ)\Lambda u \|^2 \, dt \leqq c \int_0^h \phi_n^2 \| u \|^2 \, dt \tag{16}$$

for some constant c and arbitrarily large n, $u(t) = 0$ in a neighborhood of $t = 0$.

Proof. We will first derive inequality (23) and then show that (16) and (23) are incompatible for sufficiently large n, unless $u(t) = 0$ in a neighborhood of $t = 0$. We shall write u' for du/dt etc. and shall omit displaying supscript n of ϕ_n.

We have

$$\phi[u' + (P + iQ)\Lambda u] = [(\phi u)' + iQ\Lambda\phi u] + [P\Lambda\phi u - \phi' u].$$

Squaring, we obtain

$$\begin{aligned} \phi^2 \| u' + (P + iQ)\Lambda u \|^2 &= \| (\phi u)' + iQ\Lambda\phi u \|^2 + \| P\Lambda\phi u - \phi' u \|^2 \\ &- [(\phi u)', \phi' u] - [\phi' u, (\phi u)'] + [(\phi u)', P\Lambda\phi u] + [P\Lambda\phi u, (\phi u)'] \\ &+ i[Q\Lambda\phi u, P\Lambda\phi u] - i[P\Lambda\phi u, Q\Lambda\phi u] - i[Q\Lambda\phi u, \phi' u] + i[\phi' u, Q\Lambda\phi u], \end{aligned} \tag{17}$$

where the brackets denote inner products of the functions involved. Now we integrate between 0 and h and estimate the integrals of the last eight terms. First, we have

$$[(\phi u)', \phi' u] + [\phi' u, (\phi u)'] = 2\phi'^2 \| u \|^2 + \phi\phi'[(u', u) + (u, u')],$$

and integrating between 0 and h we obtain

$$\begin{aligned} &\int_0^h \{[(\phi u)', \phi' u] + [\phi' u, (\phi u)']\} dt \\ &\quad = 2\int_0^h \phi'^2 \| u \|^2 \, dt - \int_0^h (\phi\phi'' + \phi'^2) \| u \|^2 \, dt + \phi(h)\phi'(h) \| u(h) \|^2. \end{aligned}$$

Now one verifies readily that

$$\phi\phi'' + \phi'^2 = 2\phi'^2 + \phi'^2/n$$

---

[4] Note that both F_1 and F_2 are assumed to be in C_β^∞ as functions of all their variables, t included.

and that $\phi(h)\phi'(h)\,\|u\|^2 \leqq 0$. Consequently, it follows that

$$\int_0^h [(\phi u)', \phi' u]\,dt + [\phi' u, (\phi u)']\,dt \leqq -n^{-1}\int_0^h \phi'^2\,\|u\|^2\,dt. \tag{18}$$

Next we estimate the integral of the terms $[(\phi u)', P\Lambda\phi u] + [P\Lambda\phi u, (\phi u)']$. Let us write $v = \phi u$ and P' for the operator defined by $\sigma(P') = (\partial/\partial t)\sigma(P)$ (i.e., P' is the derivative of $P(t)$). Since $\sigma(P) \in C_\beta^\infty$, $\beta > 1$ in $|z| \geqq 1$, using (10), one verifies readily that Pv is differentiable and that $(Pv)' = P'v + Pv'$. Since v is in L_1^2, it follows from Theorem 3 that Pv is in L_1^2 and ΛPv is defined. Further, since $\Lambda v = \phi\Lambda u$ is continuous, writing w for Pv, we have

$$\begin{aligned}&\{[v(t+s), \Lambda w(t+s)] - [v(t), \Lambda w(t)]\}/s\\ &\quad = [\Lambda v(t+s), (w(t+s) - w(t))/s] + [(v(t+s) - v(t))/s, \Lambda w(t)],\end{aligned}$$

and as s tends to zero, the right hand side tends towards $(\Lambda v, w') + (v', \Lambda w)$; that is, $(v, \Lambda w)$ is differentiable and its derivative is equal to the expression above. More explicitly, we have

$$(\phi u, \Lambda P\phi u)' = [\Lambda\phi u, P(\phi u)'] + [\Lambda\phi u, P'\phi u] + [(\phi u)', \Lambda P\phi u].$$

Consequently, we can write

$$\begin{aligned}&[(\phi u)', P\Lambda\phi u] + [P\Lambda\phi u, (\phi u)']\\ &= [\phi u, \Lambda P\phi u]' - [\Lambda\phi u, P'\phi u]\\ &\qquad + [(P - P^*)\Lambda\phi u, (\phi u)'] + [(\phi u)', (P\Lambda - \Lambda P)\phi u].\end{aligned}$$

Since $P = P^\#$, according to (12), the operators $(P - P^*)\Lambda$ and $P\Lambda - \Lambda P$ are bounded and their norms, as functions of t, are bounded. Also, according to (10), the norm of P' is bounded. So if we replace $(\phi u)'$ by $\phi' u + \phi u'$ above and integrate, we obtain

$$\begin{aligned}&\int_0^h [(\phi u)', P\Lambda\phi u]\,dt + [P\Lambda\phi u, (\phi u)']\,dt\\ &\geqq \phi^2(h)[u(h), \Lambda P(h)u(h)] - c\int_0^h [\phi^2\,\|\Lambda u\|\,\|u\|\\ &\qquad + |\phi\phi'|\,\|u\|^2 + \phi^2\,\|u\|\,\|u'\|]\,dt,\end{aligned} \tag{19}$$

where c is a constant independent of n. Next we have

$$\begin{aligned}&[Q\Lambda\phi u, P\Lambda\phi u] - [P\Lambda\phi u, Q\Lambda\phi u] = [(P^*Q - Q^*P)\Lambda\phi u, \Lambda\phi u]\\ &\quad = [(P^\#Q - Q^\#P)\Lambda\phi u, \Lambda\phi u] + [\Lambda(P^* - P^\#)Q\Lambda\phi u, \phi u]\\ &\qquad - [\Lambda(Q^* - Q^\#)P\Lambda\phi u, \phi u].\end{aligned} \tag{20}$$

Now, according to (12), the operators $\Lambda(P^* - P^\#)$ and $\Lambda(Q^* - Q^\#)$ are bounded and their norms, as functions of t, are bounded. Further, since $P = P^\#$ and $Q = Q^\#$ and $P \circ Q = Q \circ P$ we have

$$(P^\# Q - Q^\# P)\Lambda = (PQ - P \circ Q)\Lambda - (QP - Q \circ P)\Lambda,$$

and according to (12), the operators on the right are bounded and their norms, as function of t, are bounded. Consequently, integrating (20), we obtain

$$\int_0^h \{i[Q\Lambda\phi u, P\Lambda\phi u] - i[P\Lambda\phi u, Q\Lambda\phi u]\}dt \geqq -c\int_0^h \phi^2 \| u \| \, \| \Lambda u \| \, dt. \tag{21}$$

Finally, $i[\phi' u, Q\Lambda\phi u] - i[Q\Lambda\phi u, \phi' u] = i\phi\phi'[(\Lambda Q^* - Q\Lambda)u, u]$, and since $Q = Q^\#$, it follows again that $\Lambda Q^* - Q\Lambda$ is a bounded operator and has bounded norm. Thus, integrating, we obtain

$$\int_0^h \{i[\phi' u, Q\Lambda\phi u] - i[Q\Lambda\phi u, \phi' u]\}dt \geqq -c\int_0^h | \phi\phi' | \, \| u \|^2 \, dt. \tag{22}$$

Now we integrate (17) and using (18), (19), (21), and (22) and observing that $\phi(h) \leqq h^{-n}$, we obtain

$$\begin{aligned} \int_0^h \phi^2 \| u' + (P + iQ)\Lambda u \|^2 dt \geqq & \int_0^h \| P\Lambda\phi u - \phi' u \|^2 dt \\ & + n^{-1}\int_0^h \phi'^2 \| u \|^2 dt - c\int_0^h [| \phi\phi' | \, \| u \|^2 + \phi^2 \| u \| \, \| \Lambda u \| \\ & + \phi^2 \| u \| \, \| u' \|]dt - ch^{-2n}, \end{aligned} \tag{23}$$

where c is a constant independent of n. Now we will show that this last inequality is incompatible with (16) for sufficiently large n, unless $u(t) = 0$ in a neighborhood of $t = 0$. Assume first that $P(t)$ does not vanish identically and set

$$\int_0^h \phi'^2 \| u \|^2 dt = I^2; \qquad \int_0^h \phi^2 \| P\Lambda u \|^2 dt = \rho^2 I^2. \tag{24}$$

Then one verifies readily that, unless $u(t) = 0$ in a neighborhood of $t = 0$, we have

$$\int_0^h \phi^2 \| u \|^2 dt = o(I^2/n^2) \tag{25}$$

and $h^{2n} I^2/n^2 \to \infty$ as n tends to infinity, which implies that

$$h^{-2n} = o(I^2/n^2). \tag{26}$$

Since $P(t)$ has a two sided inverse $P(t)^{-1}$ for each t and is continuous in the norm topology for operators on L^2 (this is an immediate consequence of

(10) and our assumptions on $P(t)$), it follows that $P(t)^{-1}$ has bounded norm and, consequently, $\| \Lambda u \| \leqq c \| P\Lambda u \|$, where c is independent of t, which in turn implies that

$$\int_0^h \phi^2 \| \Lambda u \|^2 \, dt = O(\rho^2 I^2). \tag{27}$$

Since P and Q are bounded operators and have bounded norms, for those n for which (16) holds, we have from (16), (25) and (27)

$$\int_0^h \phi^2 \| u' \|^2 \, dt = O(\rho I + I/n)^2 \tag{28}$$

Finally, for the same n from (24), (25), (27), and (28), we obtain

$$\begin{gathered} \int_0^h \| P\Lambda\phi u - \phi' u \|^2 \, dt \geqq (\rho I - I)^2, \int_0^h | \phi\phi' | \, \| u \|^2 \, dt = o(I^2/n); \\ \int_0^h \phi^2 \| u \| \, \| \Lambda u \| \, dt = o(\rho I^2/n), \int_0^h \phi^2 \| u \| \, \| u' \| \, dt = o(\rho I^2/n + I^2/n^2). \end{gathered} \tag{29}$$

Now the right-hand side of (16) is larger than or equal to the right-hand side of (23) for all n for which (16) holds. Hence, for such n, from the estimates (24) to (29), we obtain

$$o(I^2/n^2) \geqq (\rho - 1)^2 I^2 + I^2/n - o(I^2/n + \rho I^2/n + I^2/n^2) - o(I^2/n^2).$$

Now, neglecting the higher order terms $o(I^2/n)$ and $o(I^2/n^2)$ multiplying by n and dividing by ρI^2 we get

$$o(1) \geqq (n(\rho - 1)^2 + 1)/\rho \geqq ((\rho - 1)^2 + 1)/\rho > \tfrac{1}{2}$$

which is, of course, impossible for sufficiently large n.

If $P(t) = 0$ identically, then (23) reduces to

$$\int_0^h \phi^2 \| u' + iQ\Lambda u \|^2 \, dt \geqq (1 + 1/n) \int_0^h \phi'^2 \| u \|^2 - c \int_0^h | \phi\phi' | \, \| u \|^2 \, dt$$

and this combined with (16), (24) and (25) gives

$$o(I^2/n^2) \geqq (1 + 1/n) I^2 - o(I^2/n)$$

which again is readily seen to be impossible for sufficiently large n. Lemma 1 is thus established.

Lemma 2. *Let $u(t)$, $0 \leqq t \leqq h$ have values in L^2 and be continuously differentiable. Then*

$$\int_0^h \phi_n^2 \| du/dt \|^2 \, dt \geqq \int_0^h \phi_n'^2 \| u \|^2 \, dt \geqq n^2 (1 + h)^{-2} \int_0^h \phi_n^2 \| u \|^2 \, dt. \tag{30}$$

Proof. To obtain the first inequality, we merely set $P = Q = 0$ in (17), integrate and use (18). The second inequality follows from the fact that $\phi_n'^2 \geqq n^2(1+h)^{-2}\phi_n^2$ in $0 \leqq t \leqq h$.

3. Uniqueness in the case of a single linear equation. Our problem consists in showing that if $u \in C_m$ is a solution of a linear homogeneous partial differential equation $A(u) = 0$ of order m, and u and its derivatives of order less than or equal to m vanish on a non-characteristic manifold M, then u must vanish in a neighborhood of M. The problem is local, and we need only consider what happens in an arbitrary neighborhood of a given point of M.

We shall consider the function u only on one side of M, and, for this purpose, it will be convenient to replace u by zero on the other, which will neither disturb the fact that u is a solution of $A(u) = 0$ nor destroy the assumed continuity properties of u. Further, and without loss of generality, we shall assume that M is of class C_m. The differential operator A will be assumed to have non-multiple characteristics, coefficients of highest order derivatives in C_β, $\beta > 1$, and remaining ones measurable and bounded. We shall first bring our differential equation to a suitable form and then replace by it an inequality involving singular operators to which, after some manipulation, we shall apply Lemma 1.

We shall denote by $k+1$ the number of independent variables. By introducing suitable coordinates $t, x_1, x_2, \cdots, x_k$, we can assume that M coincides with the paraboloid $t = |x|^2 = [\sum_1^k x_j^2]^{\frac{1}{2}}$ and that $u = 0$ in $t \leqq |x|^2$, and we shall show that $u = 0$ for $t \leqq h$, for some $h > 0$.

Since $u = 0$ in $t \leqq |x|^2$, we may freely modify the coefficients of A there, and, in fact, we shall replace A by

$$A' = g_0 A + (1 - g_0) A_0, \tag{31}$$

where g_0 is a function in C_∞ such that, $0 \leqq g_0 \leqq 1$, $g_0 = 1$ in $t \geqq |x|^2$ and $g_0 = 0$ in $t \leqq |x|^2 - \delta$, $\delta > 0$, and A_0 is the operator obtained from A by replacing its coefficients by their values at $t = x = 0$. We note that A' coincides with A at $t = x = 0$ regardless of the value of δ. By taking δ sufficiently small and by restricting our attention to a sufficiently small interval $0 \leqq t \leqq h$, we may assume that the oscillation of the coefficients of A' is less than any preassigned number ϵ. Since $t = |x|^2$ is non-characteristic, the hyperplane $t = 0$ is non-characteristic at $t = x = 0$. Consequently, we may assume that the coefficient of $\partial u^m / \partial t^m$ does not vanish in a neighborhood of $t = x = 0$. Hence, the coefficient of $\partial^m u/\partial t^m$ in A' does not vanish for $0 \leqq t \leqq h$, we may write our equation in the form

$$\partial^m u/\partial t^m + \sum_{j=1}^{m} A_j \partial u^{m-j}/\partial t^{m-j} + B(u) = 0, \tag{32}$$

where A_j is a linear partial differential operator of homogeneous order j involving only differentiations with respect to $x_1, \cdots x_k$, and $B(u)$ is linear homogeneous and of order less than m. Our previous considerations make it clear that the characteristics of (32) can be assumed to be nowhere multiple and the oscillation of the coefficients of the A_j arbitrarily small.

We shall regard the function $u(t,x)$ in (32) as a function $u(t)$ with values in $L^2(E_k)$. Since $u(t,x)$ has continuous derivatives up to order m, and vanishes for x outside a fixed bounded set, the functions

$$v_j(t) = (i\Lambda)^{m-j} d^{j-1}u/dt^{j-1}, \qquad j = 1, 2, \cdots, m, \tag{33}$$

have values in $L_1{}^2$, are continuously differentiable and the Λv_j are continuous.

Now we represent the operators A_j in (32) as in Theorem 5; that is, we set $A_j = i^j H_j \Lambda^j$, where H_j is the singular integral operator defined by

$$\sigma(H_j) = p_j(t,x,z) \,|\, z \,|^{-j},$$

$p_j(t,x,z)$ being the characteristic form of A_j. Thus (32) can be rewritten as

$$dv_m/dt + \sum_{1}^{m} H_j i\Lambda v_{m-j+1} = -B(u), \qquad dv_j/dt - i\Lambda v_{j+1} = 0, \tag{34}$$

the last equation being an immediate consequence of (33).

Now we shall write these equations in matrix form. For this purpose we shall consider $m \times m$ matrices of singular integral operators and regard them as operators acting on m-vectors with functions in $L^2(E_k)$ as components. By the norm of such a vector, we shall mean the square root of the sum of the squares of the norms of its components. The meaning of the norm of such a matrix operator is clear, and the way in which the properties of singular integral operators extend to matrix operators is also apparent. Thus, if we write $v(t)$ for the vector of components $v_1(t), v_2(t), \cdots, v_m(t)$, and $w(t)$ for $[0, 0, \cdots, -B(u)]$, and if $\mathcal{H}(t)$ denotes the matrix operator of entries $H_{lj} = -I$ (I being the identity operator) if $j = l + 1$, $H_{mj} = H_{m-j+1}$, and remaining ones equal to zero, we may write (34) as

$$dv/dt + \mathcal{H}(t) i\Lambda v = w(t). \tag{35}$$

Now we will estimate $\| w \|^2$ in terms of $\| v \|^2$. Since B is a sum of linear homogeneous partial differential operators, each of homogeneous order, applied to the derivatives $\partial^j u/\partial t^j$, representing each of these operators as in Theorem 5, we obtain

$$\| Bu \|^2 \leqq c \sum_{l+j\leqq m-1} \| \Lambda^l d^j u/dt^j \|^2 = c \sum_{l+j\leqq m-1} \| d^j \Lambda^l u/dt^j \|^2,$$

and a repeated application of Lemma 2 to each of the terms of the last sum gives

$$\int_0^h \phi_n^2 \| Bu \|^2 \leqq c \sum_j \int_0^h \phi_n^2 \| d^{m-j-1} \Lambda^j u/dt^{m-j-1} \|^2 \, dt,$$

or, according to (33), $\int_0^h \phi_n^2 \| w \|^2 \, dt \leqq c \int_0^h \phi_n^2 \| v \|^2 \, dt$. From this and (35), it follows that

$$\int_0^h \phi_n^2 \| dv/dt + \mathcal{H}(t) i\Lambda v \|^2 \, dt \leqq c \int_0^h \phi_n^2 \| v \|^2 \, dt. \tag{36}$$

In order to apply Lemma 2, we shall replace this inequality by a similar one involving a diagonal matrix instead of $\mathcal{H}(t)$.

Consider the matrix $\sigma(\mathcal{H})$ of entries $\sigma(H_{ij})$ and the characteristic polynomial $\det[\lambda I + \sigma(\mathcal{H})]$ of $-\sigma(\mathcal{H})$. Then a simple computation gives

$$\begin{aligned} &\det[\lambda I + \sigma(\mathcal{H})] \\ &\quad = \lambda^m + p_1(t,x,z) \, | z |^{-1} \lambda^{m-1} + \cdot \cdot \cdot + p_{m-1}(t,x,z) \, | z |^{-m+1} \lambda \\ &\qquad + p_m(t,x,z) \, | z |^{-m}, \end{aligned}$$

where $p_j(t,x,z)$ is the characteristic form of the operator A_j in (32). But as is readily seen, this function coincides on $| z | = 1$ with the characteristic form of the equation (32) which was assumed to be non-multiple. Consequently, for each (t,x,z), $| z | > 0$, the matrix $\sigma(\mathcal{H})$ has distinct characteristic values $\lambda_1, \lambda_2, \cdot \cdot \cdot, \lambda_m$.

Let us postpone the discussion of the cases $k = 1$ and $k = 2$, and assume temporarily that $k \geqq 3$. If $k \geqq 3$, the set of points (t,x,z), $| z | > 0$, is simply connected and the principle of monodromy implies that there exist single-value continuous functions $\lambda_1(t,x,z), \lambda_2(t,x,z), \cdot \cdot \cdot, \lambda_m(t,x,z)$ coinciding at each point with a characteristic value of $\sigma(\mathcal{H})$. Further, since the entries of $\sigma(\mathcal{H})$ are real, the $\lambda_j(t,x,z)$ which are complex can be paired in complex conjugate pairs. This implies that the imaginary part of a complex $\lambda_j(t,x,z)$ cannot vanish without the characteristics of (32) becoming multiple at a point. Hence the functions $\lambda_j(t,x,z)$ are either real or else their imaginary parts do not vanish. We note that since the entries of $\sigma(\mathcal{H})$ are functions of (t,x,z) in C_β^∞, homogeneous of degree zero with respect to z, the same holds for the $\lambda_j(t,x,z)$. Further, the oscillation of the entries of $\sigma(\mathcal{H})$ can be assumed to be arbitrarily small for each fixed z, and consequently, the same holds for the $\lambda_j(t,x,z)$.

Define now the matrix $N_1(t,x,z)$ by $N_1(t,x,z) = (a_{lj}(t,x,z))$, where $a_{lj} = \lambda_j(t,x,z)^{l-1}$. Then, since the λ_j are all distinct, N_1 is nonsingular and has an inverse. Set $N = N_1^{-1}$ and denote by D the diagonal matrix with entries $-\lambda_j(t,x,z)$ in the main diagonal. Then $\sigma(\mathcal{H})N_1 = N_1 D$, and consequently, $N\sigma(\mathcal{H}) = DN$. Let $N_0 = N(0,0,z)$ and define the matrix singular integral operators, $\mathcal{N}$, $\mathcal{N}_0$ and $\mathcal{D}$, by $\sigma(\mathcal{N}) = N$, $\sigma(\mathcal{N}_0) = N_0$, $\sigma(\mathcal{D}) = D$. Since N_0 is nonsingular, it follows from Theorem 4 that the operator $\mathcal{N}_0$ is invertible. Since the entries of $\sigma(\mathcal{N} - \mathcal{N}_0)$ and their partial derivatives with respect to coordinates of z of order $2k$ can be assumed to be arbitrarily small,[5] it follows from (10) that the norm of $\mathcal{N} - \mathcal{N}_0$ can be assumed to be arbitrarily small, and since $\mathcal{N}_0$ has an inverse $\mathcal{N} = \mathcal{N}(t)$ has an inverse with bounded norm. Consequently,

$$\int_0^h \phi_n^2 \, \| \mathcal{N} dv/dt + \mathcal{N}\mathcal{H} i\Lambda v \|^2 \, dt \leqq c \int_0^h \phi_n^2 \, \| dv/dt + \mathcal{H} i\Lambda v \|^2 \, dt$$

and $\int_0^h \phi_n^2 \, \| v \|^2 \, dt \leqq c \int_0^h \phi_n^2 \, \| \mathcal{N} v \|^2 \, dt$, and from (36), we obtain

$$\int_0^h \phi_n^2 \, \| \mathcal{N} dv/dt + \mathcal{N}\mathcal{H} i\Lambda v \|^2 \, dt \leqq c \int_0^h \phi_n^2 \, \| \mathcal{N} v \|^2 \, dt. \tag{37}$$

Now $\sigma(\mathcal{N})$ is a function of (t,x,z) of C_β^∞, $\beta > 1$ in $|z| \geqq 1$. Consequently, if we define $d\mathcal{N}/dt$ by $\sigma(d\mathcal{N}/dt) = \partial\sigma(\mathcal{N})/\partial t$, then $d\mathcal{N}/dt$ has bounded norm and

$$\mathcal{N} dv/dt = d(\mathcal{N} v)/dt - (d\mathcal{N}/dt)v = d(\mathcal{N} v)/dt + v', \tag{38}$$

where $\| v' \| \leqq c \, \| v \|$, and consequently, also $\| v' \| \leqq c \, \| \mathcal{N} v \|$. Further, since

$$\sigma(\mathcal{N})\sigma(\mathcal{H}) = N\sigma(\mathcal{H}) = DN = \sigma(\mathcal{D})\sigma(\mathcal{N}),$$

we have $\mathcal{N} \circ \mathcal{H} = \mathcal{D} \circ \mathcal{N}$ and

$$\begin{aligned} \mathcal{N}\mathcal{H} i\Lambda = \mathcal{D} i\Lambda\mathcal{N} &+ \mathcal{D} i(\mathcal{N}\Lambda - \Lambda\mathcal{N}) \\ &+ (\mathcal{D} \circ \mathcal{N} - \mathcal{D}\mathcal{N}) i\Lambda + (\mathcal{N}\mathcal{H} - \mathcal{N} \circ \mathcal{H}) i\Lambda. \end{aligned}$$

But according to Theorem 3, the last three terms on the right represent bounded operators, and consequently, we may write

$$\mathcal{N}\mathcal{H} i\Lambda v = \mathcal{D} i\Lambda\mathcal{N} v + v'', \tag{39}$$

---

[5] Note that the oscillations of the entries of this matrix and of its derivatives with respect to coordinates of z can be estimated in terms of the oscillation of the coefficients of the equation (32).

where $\| v'' \| \leqq c \| v \|$, and therefore, also $\| v'' \| \leqq c \| \mathfrak{N} v \|$. Substituting (38) and (39) in (37), we obtain

$$\begin{aligned}(40)\qquad &\int_0^h \phi_n^2 \| d(\mathfrak{N}v)/dt + \mathfrak{D} i\Lambda(\mathfrak{N}v) \|^2 dt \leqq c \int_0^h \phi_n^2 \| \mathfrak{N} v \|^2 dt \\ &+ c\int_0^h \phi_n^2 \| v' \|^2 dt + c \int_0^h \phi_n^2 \| v'' \|^2 dt \leqq c \int_0^h \phi_n^2 \| \mathfrak{N} v \|^2 dt.\end{aligned}$$

Let now $w_1, w_2, \cdots, w_m$ be the components of $\mathfrak{N} v$, and $P_1 + iQ_1$, $P_2 + iQ_2$, $\cdots, P_m + iQ_m$ the entries in the main diagonal if $i\mathfrak{D}$, where $-\sigma(Q_j)$ and $\sigma(P_j)$ are, respectively, equal to the real and imaginary part of $\lambda_j(t,x,z)$. Since the imaginary part of $\lambda_j(t,x,z)$ is identically zero or else does not vanish, and since the oscillation of $\lambda_j(0,0,z) - \lambda_j(t,x,z)$ and its derivatives with respect to coordinates of z of order $2k$ can be assumed to be arbitrarily small, it follows from (10) and Theorem 4, that either P_j vanishes identically or else has an inverse. Thus (40) can be written as

$$(41)\qquad \int_0^h \phi_n^2 \| dw_j/dt + (P_j + iQ_j)\Lambda w_j \|^2 dt \leqq c \sum_{i=1}^m \int \phi_n^2 \| w_i \|^2 dt, \qquad j = 1, 2, \cdots, m.$$

Let now j, $1 \leqq j \leqq m$, be an index such that

$$(42)\qquad \int_0^h \phi_n^2 \| w_j \|^2 dt \geqq 1/m \int_0^h \phi_n^2 \sum_{l=1}^m \| w_l \|^2 dt$$

for infinitely many n. Then for such an index, (41) yields

$$\int_0^h \phi_n^2 \| dw_j/dt + (P_j + iQ_j)\Lambda w_j \|^2 dt \leqq c \int_0^h \phi_n^2 \| w_j \|^2 dt$$

for infinitely many n. Now, as is readily verified, the remaining assumptions of Lemma 1 are satisfied, and thus $w_j(t) = 0$ in a neighborhood of $t = 0$. But then (42) implies that all the other components of $w = \mathfrak{N} v$ must vanish in the same interval. Consequently, $\mathfrak{N} v = 0$ for t sufficiently small, whence $v = 0$ and $u = 0$ for the same values of t.

Thus uniqueness is established, provided $k \geqq 3$.

To complete the proof in the cases $k = 1$ and $k = 2$, we still have to construct the functions $\lambda_j(t,x,z)$ coinciding at each point with a characteristic value of $\sigma(\mathfrak{A})$. If $k = 1$, the set of points (t,x,z), $|z| > 0$, has two simply connected components. On each of these, we can construct the functions $\lambda_j(t,x,z)$ as we did in the case $k \geqq 3$, and they will turn out to be either real or else have a non-vanishing imaginary part. Then we pair the functions on each component in such a way that $\lambda_j(t,x,z) = -\lambda_j(t,x,-z)$

and this will yield the functions $\lambda_j(t,x,z)$ over the whole set (t,x,z), $|z|>0$, with the desired property of either being real or else having a non-vanishing imaginary part.

If $k=2$, the set of points (t,x,z), $|z|>0$, is no longer simply connected; i.e., the principle of monodromy does not hold, and indeed, it is possible to construct a differential operator for which no continuous single valued functions $\lambda_j(t,x,z)$ exist. For such an operator, our argument can be carried no further and the question of uniqueness remains open. Yet, in a special case which is certainly not devoid of interest, the functions $\lambda_j(t,x,z)$ still exist. This is when there exist at most two complex characteristic values of $\sigma(\mathfrak{A})$ at each point (t,x,z), $|z|>0$. To show the existence of the $\lambda_j(t,x,z)$, we first construct the functions $\lambda_j(t,x,y)$ on the universal covering space of the set (t,x,z), $|z|>0$. The same argument used previously shows that either $\lambda_j(t,x,y)$ is real at all points or else its imaginary part does not vanish. Let us denote by λ_1 and λ_2 the two complex λ_j and assume that at (t_0,x_0,y_0), $\mathrm{Im}[\lambda_1]>0, \mathrm{Im}[\lambda_2]<0, \lambda_3<\lambda_4<\cdots<\lambda_m$. Since the λ_j are distinct at each point, these inequalities hold everywhere on the covering space. Now if (t_1,x_1,y_1) and (t_2,x_2,y_2) are two points above the same point (t,x,z), then the sets of values of the λ_j at these points coincide. Since the inequalities above hold at both (t_1,x_1,y_1) and (t_2,x_2,y_2), it follows that $\lambda_j(t_1,x_1,y_1)=\lambda_j(t_2,x_2,y_2)$, $j=1,2,\cdots,m$, and consequently, the functions $\lambda_j(t,x,y)$ can be lifted to the set (t,x,z), $|z|>0$, which proves our assertion.

To conclude, we note that there will be at most two complex λ_j if the order of the equation does not exceed 3. Consequently, there is uniqueness of solutions of the Cauchy problem for second and third order equations with non-multiple characteristics, regardless of the number of independent variables.

Our results on a single equation can be summarized in the following

THEOREM 6. *Let $A(u)=0$ be a linear partial differential equation of order m in a function u of k variables. Let the coefficients of derivatives of order m be real and in C_β, $\beta>1$, and the remaining ones measurable and bounded. Then if the characteristics of the equation are non-multiple,*[5a] *solutions of the Cauchy problem are unique in C_m, provided that $k\neq 3$ or $m\leqq 3$.*

[5a] Although not strictly necessary, here as well as in Theorem 7 we assume the characteristic form to be free of multiplicities in the complex domain.

4. Uniqueness in the case of a system of linear equations. With a few changes, the method used in the preceding section can be applied to a system of equations.

Assume that we have a system of r equations in r functions $u_1, u_2, \cdots, u_r$. Then we regard the functions u_j as the components of a vector function u and the system of equations as a single equation in u with $r \times r$ matrices as coefficients. After bringing the equation to the form (32), we can proceed as before. The v_j in (33) will now be r-vectors and the $v(t)$ in (35) an mr-vector. The matrix $\mathcal{H}(t)$ in (35) will become an $m \times m$ matrix with $r \times r$ matrices as entries, that is, an ordinary $mr \times mr$ matrix. The characteristic polynomial of $-\sigma(\mathcal{H})$ will coincide on $|z| = 1$ with the characteristic form of the system, and the characteristic value functions can be constructed as before.

So far, the way in which we have to modify the argument of the preceding section is obvious. But in trying to construct the matrix N_1 with the property that

$$\sigma(\mathcal{H}) N_1 = N_1 D, \tag{43}$$

where D is diagonal, we run into topological difficulties which we know how to overcome only by imposing an additional restriction on the number of independent variables, or else, by assuming that both the system and the u_j are sufficiently differentiable, which enables us to obtain by differentiation another system where such difficulties do not appear. Observe that if (43) is to be satisfied, the column vectors of N_1 must be eigenvectors of $\sigma(\mathcal{H})$ corresponding to its distinct characteristic values. In the case of a single equation, given the simple form of $\sigma(\mathcal{H})$, these eigenvector functions, as we have seen, can be constructed easily in terms of the corresponding characteristic value functions. In the case of a system, though, such an obvious construction does not seem to be available and we are forced to resort to topological techniques. Given a characteristic value function $\lambda_j(t, x, z)$ of $-\sigma(\mathcal{H})$ (in the general case it will be a complex valued function), to each point (t, x, z), $|z| > 0$, there corresponds a one dimensional subspace of the mr-dimensional complex Euclidean space, namely, the corresponding eigenspace of the matrix $\sigma(\mathcal{H})$. Our problem is then to select at each point (t, x, z), $|z| > 0$, a non-zero vector from this eigenspace so as to obtain a continuous eigenvector function corresponding to the characteristic value function $\lambda_j(t, x, z)$. Since the entries of $\sigma(\mathcal{H})$ as functions of (t, x, z) are homogeneous of degree zero with respect to z, it will be sufficient to carry out the construction for $|z| = 1$. Further, since the oscillation of the coefficients of the equations can be assumed to be arbitrarily small it will be enough to construct the eigenvector function, denote it momentarily by $w_j(t,x,z)$, for $(t,x,z)=(0,0,z)$, $|z|=1$, and then extend it to all (t,x,z), $|z|=1$, by imposing the condition that the Hermitian inner product of $w_j(t,x,z)$ and $w_j(0,0,z)$ be real and positive.

Consider the rm-dimensional complex Euclidean space, its unit sphere S, and the collection P_{rm-1} of all its one dimensional subspaces. Then P_{rm-1} can be regarded as the $(rm-1)$-dimensional complex projective space, and S can be thought of as a fibre bundle over P_{rm-1}. The fibre over each point of P_{rm-1} is the intersection of the corresponding subspace of our Euclidean space with S, i.e., a 1-sphere; the group is the complexes of absolute value 1 (see [12], page 106). We are given a continuous mapping ϕ of the set of points $(0,0,z)$, $|z|=1$, that is, of S_{k-1}, into P_{rm-1} and we want to select continuously a vector in S belonging for each $(0,0,z)$ to the one-dimensional space corresponding to $\phi(0,0,z)$. For this purpose, consider the bundle over S_{k-1} induced by the mapping $\phi\colon S_{k-1}\to P_{rm-1}$ (see [12], page 47). This induced bundle is a 1-sphere bundle over S_{k-1} with the complexes of absolute value 1 as group. But then, if $k-1\neq 2$, there exists a cross section (see [12], page 99); that is, there exists a continuous mapping $\psi(0,0,z)$ of S_{k-1} into S such that for each z the unit vector $\psi(0,0,z)$ is contained in the one dimensional space corresponding to $\phi(0,0,z)$. This mapping can be assumed, in addition, to be in C^∞ (see [12], page 25).

Once the eigenvector functions of the matrix $\sigma(\mathfrak{A})$ corresponding to each characteristic value function $\lambda_j(t,x,z)$ have been constructed, we can obtain without difficulty the matrix N_1 in (43), and from here on the argument proceeds exactly as in the preceding section.

If the equations in the system have sufficiently differentiable coefficients and the functions $u_1,u_2,\cdots,u_r$ are also sufficiently differentiable it is possible to avoid the topological difficulty discussed above, and consequently, drop the additional restriction $k\neq 3$.

We note that if the functions $u_1,u_2,\cdots,u_r$ and their derivatives of orders less than or equal to $m-1$ vanish on a non-characteristic manifold M and can be further differentiated continuously n times, and if the coefficients of the equations have continuous derivatives up to order $n-1$, then all the derivatives of the u_j of orders less than or equal to $m+n-1$ vanish on M. This means that if we replace our system of equations by another obtained from this one by differentiation, the Cauchy data of the new system will still vanish.

Consider a linear differential operator $A(u)$ of order m with $r\times r$

matrices as coefficients and thought of as acting on vector valued functions $u = (u_1, u_2, \cdots, u_r)$ in the variables $x_1, x_2, \cdots, x_k$. With the notation used in Theorem 5, let a_α be the coefficient of D_α, and let $\pi(A)$ be the $r \times r$ matrix $\pi(A) = \sum_\alpha a_\alpha z^\alpha$, where z^α runs over all monomials in $z_1, z_2, \cdots, z_k$ of degree m. This matrix we shall call the characteristic matrix of A. The polynomial in z with functions of $x = (x_1, x_2, \cdots, x_k)$ as coefficients given by $p(A) = \det[\sum_\alpha a_\alpha z^\alpha]$ coincides with the characteristic form of A.

Let now A_1 and A_2 be two operators as above. Then $\pi(A_1 + A_2) = \pi(A_1) + \pi(A_2) \neq 0$ unless $A_1 + A_2$ is of order less than m, in which case, $\pi(A_1) + \pi(A_2) = 0$. Further, if $A_1 A_2$ is defined, $\pi(A_1 A_2) = \pi(A_1)\pi(A_2)$.

If $\det[\lambda I - \pi(A)] = \lambda^r + b_1\lambda^{r-1} + \cdots + b_{r-1}\lambda + b_r$ is the characteristic polynomial of the matrix $\pi(A)$, then the b_j are homogeneous polynomials in z of degrees jm with functions of x as coefficients. Since a matrix satisfies its own characteristic equation, we have

$$\pi(A)^r + b_1\pi(A)^{r-1} + \cdots + b_{r-1}\pi(A) + b_r I = 0. \tag{44}$$

Let now B_j be the differential operator of homogeneous order mj with characteristic matrix $b_j I$ (I being the unit matrix). Then (44) implies that

$$A^r + \sum_1^r B_j A^{r-j} = R$$

is of order less than mr. Consequently, if $A(u) = 0$, then

$$B_r(u) = R(u) - (A^{r-1} + \sum_1^{r-1} B_j A^{r-j-1}) A(u) = R(u). \tag{45}$$

The matrix B_r is diagonal and its entries on the main diagonal are all identical and equal to an ordinary (in contrast with the matrix differential operators) partial differential operator, denote it by B, which is of homogeneous order rm and whose characteristic form is $\det[\pi(A)]$, that is, coincides with the characteristic form of A. In terms of components, equation (45) can be written as $B(u_j) = R_j(u_1, \cdots, u_r)$, $j = 1, 2, \cdots, r$, where B is of order mr and has non-multiple characteristics and the R_j are of lower order.

Now the reader will have little difficulty in verifying that the argument used in the preceding section applies also to systems in which the principal part of each equation contains just one function u_j, as is the case with the system above.

We omit further details and summarize our results in the following

THEOREM 7. *Let $A(u)$ be a system of r linear partial differential equations of order m in r functions u_j of k variables. Then if the characteristics of the system are non-multiple:*[5a] i) *solutions of the Cauchy problem are unique in C_m, provided that the coefficients of derivatives of order m are real and in C_β, $\beta > 1$, the remaining ones are measurable and bounded, and $k = 2$ or $k > 4$;* ii) *solutions of the Cauchy problem are unique in C_{rm}, provided that the coefficients of derivatives of order m are real and in $C_{m(r-1)}$, the remaining ones are in $C_{m(r-1)}$, and $mr \leqq 3$ or $k \neq 3$.*

5. Uniqueness in the non-linear case. The argument by which one extends the results on uniqueness to the non-linear case is well known. We shall briefly discuss the case of a single equation. Systems are treated in exactly the same way.

Let $F(x, u, u_\alpha) = 0$ be a partial differential equation, x denoting the point $x_1, x_2, \cdots, x_k$, and u_α running over the derivatives of the function u of order less than or equal to m, and assume that F is of class C_3.

Let u and v be two solutions with the property that $u - v$ and its derivatives of order less than or equal to $m - 1$ vanish on a non-characteristic manifold M, and assume that u and v are of class C_{m+2}. Denote by F_u and F_α the partial derivatives of F with respect to u and u_α respectively. Then $F(x, u, u_\alpha) = F(x, v, v_\alpha) = 0$ and by the mean value theorem,

$$F(x, u, u_\alpha) - F(x, v, v_\alpha) = (u - v) \int_0^1 F_u[x, v + (u - v)s, v_\alpha + (u_\alpha - v_\alpha)s]\,ds$$

$$+ \sum_\alpha (u_\alpha - v_\alpha) \int_0^1 F_\alpha[x, x + (u - v)s, v_\alpha + (u_\alpha - v_\alpha)s]\,ds = 0.$$

If we now replace u, v, u_α and v_α by their values as functions of x in the integrals on the right, we find that $u - v$ satisfies a linear differential equation for which M is non-characteristic. Further, given the differentiability properties of F, u, and v, one verifies readily that the coefficients of this equation are in C_2. From our previous results and assuming non-multiplicity of the characteristics of the equation, it follows that $u - v = 0$ in a neighborhood of M.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.
CORNELL UNIVERSITY.

REFERENCES.

[1] N. Aronszajn, " Sur l'unicité du prolongement des solutions des équations aux dérivées partielles elliptiques du second ordre," *Comptes Rendus*, vol. 242 (1956), pp. 723-725.

[2] T. Carleman, " Sur un problem d'unicité pour les systèmes d'équations aux dérivées partielles à deux variables indépendentes," *Arkiv för Mathematik*, vol. 26B, no. 17 (1939), pp. 1-9.

[3] E. de Giorgi, " Un esempio di non-unicità della soluzione del problema di Cauchy, relativo ad una equazione differenziale lineare a derivate parziali di tipo parabolico," *Rendiconti di Matematica e della une Applicazioni*, ser. 5, vol. 14 (1955), pp. 382-387.

[4] P. Hartman and A. Wintner, " On the local behaviour of solutions of non-parabolic partial differential equations. III. Approximations by spherical harmonics," *American Journal of Mathematics*, vol. 77 (1955), pp. 453-483.

[5] E. Heinz, " Ueber die Eindeutigkeit beim Cauchyschen Anfangswertproblem einer elliptischen Differentialgleichung zweiter Ordnung," *Nachrichten der Akademie der Wissenschaften in Göttingen*, no. 1 (1955), pp. 1-12.

[6] E. Holmgren, " Ueber Systeme von linearen partiellen Differentialgleichungen," *Ofversigt af Kongl. Vetenskaps Akamemiens Förhandlingar*, vol. 58 (1901), pp. 91-103.

[7] P. D. Lax, "A stability theorem for solutions of abstract differential equations, and its application to the study of the local behaviour of solutions of elliptic equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1956), pp. ———.

[8] C. Müller, " On the behaviour of the solutions of the differential equations $u' = F(x, u)$ in the neighborhood of a point," *Communications on Pure and Applied Mathematics*, vol. 7 (1954), pp. 505-515.

[9] L. Nirenberg, " Uniqueness for the Cauchy problem for differential equations with constant leading coefficients," to appear in the *Communications on Pure and Applied Mathematics.*

[10] A. Plis, " The problem of uniqueness for the solution of a system of partial differential equations," *Bulletin de l'Académie Polonaise des Sciences*, vol. 2 (1954), pp. 55-57.

[11] A. P. Calderón and A. Zygmund, " Singular integral operators and differential equations," *American Journal of Mathematics*, vol. 79 (1957), pp. 901-921.

[12] N. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

$N \times N$ MATRICES OVER AN AW^*-ALGEBRA.[†]

By S. K. Berberian.

Introduction. The object of this paper is to prove the following conjecture of I. Kaplansky: if A is any AW^*-algebra, the algebra A_n of $n \times n$ matrices over A is AW^*. This result is readily accessible in all but one (namely finite type II) of the types according to which AW^*-algebras are ordinarily classified ([4], Theorems 4.2, 4.6). These known results may be summarized as follows.

After decomposing A into the direct sum of a type I algebra and a continuous algebra (i.e., one which contains no abelian projections), these two cases may be considered separately. If A is type I, then A can be realized as the algebra of all bounded module operators on a suitable AW^*-module H ([6], Theorem 8). Evidently, A_n is the algebra of all bounded module operators on the direct sum of n copies of H and, hence, is an AW^*-algebra of type I ([6], Theorem 7).

Suppose next that A is continuous. After decomposing A as the direct sum of a properly infinite algebra (i.e., one without finite direct summand), and a finite algebra (necessarily of type II), these two cases may be considered separately. If A is properly infinite, one can find n orthogonal projections $e_1, \cdots, e_n$ in A, with sum 1, each equivalent to 1 ([4], Lemma 4.5). By standard matrix unit techniques (see [5], Section 5), A is *-isomorphic with the $n \times n$ matrix algebra $(e_1Ae_1)_n$. Say $w^*w = e_1$, $ww^* = 1$. Then $a \rightarrow w^*aw$ is a *-isomorphism of A onto e_1Ae_1; this lifts to a *-isomorphism of A_n onto $(e_1Ae_1)_n$, thus A_n is *-isomorphic with the AW^*-algebra A itself.

Thus, we are concerned primarily with the finite type II case. The first step is to show, using the regular ring of A, that A_n is a B_p^*-algebra. At this point Kaplansky showed that A_n is AW^* provided A is a factor; in the general case, our proofs of generalized comparibility and finiteness are modeled on Kaplansky's arguments.

1. Preliminaries. All C^*-algebras to be considered have unity elements. It is appropriate to mention that if B is any C^*-algebra, B_n is also a C^*-

---

[†] Received July 10, 1957.

algebra. This is easily seen by representing B as a uniformly closed *-algebra of operators on a Hilbert space H; then B_n is a uniformly closed *-algebra of operators on the direct sum of n copies of H. This representation shows that if $x = (a_{ij}) \in B_n$, then $\| a_{ij} \| \leqq \| x \|$ for all i, j. On the other hand, $\| x \| \leqq n^2 \max \| a_{ij} \|$, as one sees by expresssing x as the sum of n^2 matrices, each containing at most one non-zero entry. These remarks yield the following useful fact: if (B_α) is any family of C^*-algebras with C^*-sum B, then B_n is the C^*-sum of the $(B_\alpha)_n$ (see [4], Section 2, for a discussion of C^*-sums).

For the remainder of the paper, A is an AW^*-algebra with center Z, n is a fixed natural number, and A_n is the C^*-algebra of $n \times n$ matrices over A. At times we shall identify A with the subalgebra of A_n consisting of the "scalar" matrices $(a\delta_{ij})$, $a \in A$; thus if $x = (a_{ij}) \in A_n$, $ax = (aa_{ij})$ and $xa = (a_{ij}a)$. The center of A_n consists of the scalar matrices $(c\delta_{ij})$, $c \in Z$; thus, when A is identified with the scalar subalgebra of A_n, Z becomes the center of A_n. In particular, the center of A_n is an AW^*-algebra. The first part of the next lemma relates the LUB of central projections to the rest of A_n.

LEMMA 1.1. *Let (h_α) be a family of central projections in the AW^*-algebra A.*

(1) *If $x \in A_n$, $h_\alpha x = 0$ for all α, and $h = \mathrm{LUB}\, h_\alpha$ (computed in Z), then $hx = 0$.*

(2) *If the h_α are orthogonal, and $\mathrm{LUB}\, h_\alpha = 1$, then A_n is the C^*-sum of the $h_\alpha A_n = (h_\alpha A)_n$; if moreover each $h_\alpha A_n$ is AW^*, so is A_n.*

Proof. (1) Say $x = (a_{ij})$. Then $0 = h_\alpha x = (h_\alpha a_{ij})$, thus $h_\alpha a_{ij} = 0$ for all indices; hence $ha_{ij} = 0$. (2) Since A is the C^*-sum of the $h_\alpha A$ ([4], Lemma 2.5), A_n is the C^*-sum of the $(h_\alpha A)_n$ by the earlier remarks. The last assertion of the lemma follows from the fact that the C^*-sum of AW^*-algebras is AW^* ([4], Section 2).

This lemma, of course, justifies the consideration of cases in the Introduction. Another programming for the consideration of cases is as follows. Decompose A into a finite algebra and a properly infinite algebra. After disposing of the properly infinite part by the argument in the Introduction, we may assume A to be finite, and decompose it into parts of type I and type II. The type I case reduces, by Lemma 1.1, to the homogeneous case ([5], Lemma 18), i.e., to the case that A is an $m \times m$ matrix algebra over its center Z ([3], Lemme 4.2); then A_n is the $mn \times mn$ matrix algebra over Z. Thus the finite type I case is reduced to the case that A is commutative, and this is settled as a very special case of ([6], Theorem 7).

2. The regular ring. Henceforth, the AW^*-algebra A is assumed to be finite. Identifying A as a $*$-subalgebra of its regular ring C ([1], Theorem 2.1), A_n becomes a $*$-subalgebra of C_n.

LEMMA 2.1. *If* $x, y, z \in C_n$, *and* $x^*x + y^*y + z^*z = 1$, *then* $x, y, z \in A_n$.

Proof. Say $x = (x_{ij})$, $y = (y_{ij})$, $z = (z_{ij})$. Then

$$\sum_k (x_{ki}^* x_{ki} + y_{ki}^* y_{ki} + z_{ki}^* z_{ki}) = 1$$

for $i = 1, \cdots, n$; hence $x_{ki}, y_{ki}, z_{ki} \in A$ by ([1], Lemma 5.1).

In particular, $x^*x = 0$ implies $x = 0$, thus C_n is *$*$-regular*, as observed in the proof of ([1], Corollary 7.7). Also, A_n contains all the partial isometries of C_n ([1], Section 11), and A_n is a *B_p^*-algebra* ([1], Corollary 7.7). Next, we establish polar decomposition in A_n.

LEMMA 2.2. *Every* $x \in A_n$ *has a factorization* $x = wr$, $r \geqq 0$, $r^2 = x^*x$, $w^*w = RP(x)$, $ww^* = LP(x)$. *In particular,* $LP(x) \sim RP(x)$.

Proof. Let r be the positive square root of x^*x in the C^*-algebra A_n. Let $e = RP(x)$, $f = LP(x)$. Since $RP(x) = RP(x^*x) = RP(r^2) = RP(r)$, we have $C_n e = C_n x = C_n r$; hence $x = wr$ for some $w \in C_n$. Since $x = wr = w(er) = (we)r$, we may assume $we = w$. Then $w^*w = e$, $ww^* = f$ by the same argument as in ([2], Lemma 3.3). Quoting ([2], Corollary 3.4), we have

COROLLARY 2.3. *For any two projections* $e, f \in A_n$,

$$e \cup f - f \sim e - e \cap f.$$

COROLLARY 2.4. *For any two projections* $e, f \in A_n$, *there exist orthogonal decompositions* $e = e' + e''$, $f = f' + f''$, *such that* $e' \sim f'$ *and* $e''f = f''e = 0$.

Proof. Set $e' = LP(ef)$, $f' = RP(ef)$, $e'' = e - e'$, $f'' = f - f'$.

Remarks.

(1) Any *sequence* of projections $e_1, e_2, e_3, \cdots \in A_n$ has a LUB. Specifically, LUB $e_i = RP(x)$, where $x = \sum 2^{-i} e_i$ (convergent in norm; see the proof of [7], Theorem 5.8).

(2) To show that A_n is AW^*, it suffices to prove that every family of orthogonal projections (e_i) has a LUB.

3. Generalized comparability. Projections e, f in a C^*-algebra B are said to be *very orthogonal* in case there is a central projection h such that $e \leqq 1 - h$, $f \leqq h$. B is said to have *generalized comparability* if, for every pair of projections e, f, there exists a central projection h such that $he \prec hf$ and $(1-h)f \prec (1-h)e$; equivalently, there exist orthogonal decompositions $e = e' + e''$, $f = f' + f''$, such that $e' \sim f'$ and e'', f'' are very orthogonal.

As in the preceding section, A is a finite AW^*-algebra. It will be shown that A_n has generalized comparability. We denote the diagonal matrix units of A_n by $u_1, \cdots, u_n$; thus $u_k = (\delta_{ik}\delta_{kj})$, and $u_1 + \cdots + u_n = 1$. The u_k are, of course, mutually equivalent, and the mapping $a \to (a\delta_{ik}\delta_{kj})$ is a $*$-isomorphism of A onto $u_k A_n u_k$.

LEMMA 3.1. *Given any projection $e \in A_n$, there exists an orthogonal decomposition $e = e_1 + \cdots + e_n$ such that $e_k \prec u_1$ $(k = 1, \cdots, n)$.*

Proof. We give the proof for $n = 3$. Applying Corollary 2.4 to the pair e, u_1, we have decompositions $e = e_1 + f$, $u_1 = u + v$ with $e_1 \sim u$ and $fu_1 = 0$. Thus $e_1 \prec u_1$ and $f \leqq 1 - u_1 = u_2 + u_3$. Then apply Corollary 2.4 to the pair f, u_2 to obtain decompositions $f = e_2 + e_3$, $u_2 = a + b$, with $e_2 \sim a$ and $e_3 u_2 = 0$. Thus, $e_2 \prec u_2$ and $e_3 \leqq 1 - u_2 = u_1 + u_3$. Since also $e_3 \leqq f \leqq u_2 + u_3$, we have $e_3 \leqq (u_1 + u_3)(u_2 + u_3) = u_3$. Thus $e = e_1 + e_2 + e_3$, where $e_1 \prec u_1$, $e_2 \prec u_2$, $e_3 \leqq u_3$.

LEMMA 3.2. *If $e, f \in A_n$ are projections such that $e \prec u_1$ and $f \prec u_1$, then e, f are generalized comparable.*

Proof. The algebra $u_1 A_n u_1$, being isomorphic with A, has generalized comparability; its projections are simply those of A_n which are $\leqq u_1$. Since the center of A_n is isomorphic with that of $u_1 A_n u_1$ (via the mapping $z \to z u_1$), it is clear that two subprojections of u_1 are generalized comparable in $u_1 A_n u_1$ if and only if they are generalized comparable in A_n.

By assumption, $e \sim e' \leqq u_1$, $f \sim f' \leqq u_1$. If h is a central projection such that $he' \prec hf'$ and $(1-h)f' \prec (1-h)e'$ ([4], Theorem 5.6), evidently, $he \sim he' \prec hf' \sim hf$ and $(1-h)f \sim (1-h)f' \prec (1-h)e' \sim (1-h)e$; thus, $he \prec hf$ and $(1-h)f \prec (1-h)e$.

LEMMA 3.3. *A_n has generalized comparability.*

Proof. Given two projections $e, f \in A_n$, we seek decompositions $e = e' + e''$, $f = f' + f''$, such that $e' \sim f'$, and e'', f'' are very orthogonal; thus we are always free to throw away equivalent subprojections of e, f.

We illustrate the proof with $n = 3$. By Lemma 3.1, we have decompositions $e = e_1 + e_2 + e_3$, $f = f_1 + f_2 + f_3$, with all summands $\prec u_1$. Applying Lemma 3.2 to the pair e_1, f_1, and throwing away equivalent subprojections, we can assume that e_1, f_1 are orthogonal. Continuing, we may assume every pair e_i, f_j to be very orthogonal; but then it is clear that e, f are very orthogonal.

4. Finiteness.

A C^*-algebra is *finite* if the relation $e \sim 1$ implies $e = 1$ ([3], Définition 4.1). If B is a C^*-algebra, a projection $e \in B$ is said to be finite in case the C^*-algebra eBe is finite; equivalently, the relations $f \leqq e$, $f \sim e$ imply $f = e$. We shall show in this section that A_n is finite (we are assuming A is finite).

Using Lemma 1.1(1), the proof of ([4], Theorem 4.2) goes through for A_n, and we conclude that A_n is, at any rate, the direct sum of a finite algebra and an algebra without finite central projections.

LEMMA 4.1. *If A is a finite AW^*-algebra, then A_n is finite.*

Proof. Let $u_1, \cdots, u_n \in A_n$ be as in the preceding section. Since $u_k A_n u_k$ is $*$-isomorphic with the finite algebra A, u_k is a finite projection. Since $u_1 + \cdots + u_n = 1$, it will suffice to prove the following: if $e, f \in A_n$ are finite projections, so is $e \cup f$. This can be proved exactly as in ([4], Theorem 6.2; the relations in the last line of the proof should read $g \prec e$ and $1 - g \prec 1 - e$). We mention that in the crucial ([4], Lemma 4.5), only countable LUB's are needed.

5. Finite type II.

In this section, we assume that the finite AW^*-algebra A is type II.

LEMMA 5.1. *Any projection $e \in A_n$ has an orthogonal decomposition $e = e' + e''$ with $e' \sim e''$.*

Proof. By Lemma 3.1, write $e = e_1 + \cdots + e_n$ with $e_k \prec u_1$ for all k. Say $e_k \sim f_k \leqq u_1$. Since $u_1 A_n u_1$ is a continuous AW^*-algebra, $f_k = f_k' + f_k''$ with $f_k' \sim f_k''$. The equivalence $f_k \sim e_k$ induces a decomposition $e_k = e_k' + e_k''$; the projections $e' = e_1' + \cdots + e_n'$ and $e'' = e_1'' + \cdots + e_n''$ have the required properties.

A non-zero projection e is called *fundamental*, of *order* $k = 2^m$, if there exists a central projection h and an orthogonal decomposition $h = e_1 + \cdots + e_k$ such that $e \sim e_i$ for all i ([3], Définition 6.1). From Lemma 5.1, it results that given any non-zero central projection $h \in A_n$, and any integer $m \geqq 0$, h contains a fundamental projection of order 2^m. By ([3], Lemma

4.4), the order of a fundamental projection, as well as the associated central projection, is unique.

LEMMA 5.2. *Every non-zero projection* $e \in A_n$ *contains a fundamental projection.*

Proof. Since $e = eu_1 + \cdots + eu_n$, suppose, for example, that $eu_1 \neq 0$. Let $e' = LP(eu_1)$, $f' = RP(eu_1)$, so that $e' \sim f' \leqq u_1$. Since $u_1 A_n u_1$ is isomorphic with A, f' contains a fundamental projection f'' ([3], Lemme 6.4). The equivalence $f' \sim e'$ carries f'' into a fundamental projection e'', $e'' \leqq e' \leqq e$.

LEMMA 5.3. *Every non-zero projection* $e \in A_n$ *has the form* $e = \mathrm{LUB}\, e_i$, *with* (e_i) *a family of orthogonal fundamental projections.*

Proof. Let (e_i) be a maximal family of orthogonal fundamental projections $\leqq e$. If $f \in A_n$ is a projection such that $e_i \leqq f$ for all i, it must be shown that $e \leqq f$. If on the contrary, $x = e(1-f) \neq 0$, then $e(1-f)e = x^*x \neq 0$. By spectral theory, $e(1-f)ey = g$ is a non-zero projection, for suitable $y \in A_n$ ([4], Lemma 2.1). Since $eg = g$, $g \leqq e$. By Lemma 5.2, let h be a fundamental projection, $h \leqq g$. For any i,

$$e_i h = e_i g h = e_i e(1-f)eyh = e_i(1-f)eyh = (e_i - e_i f)eyh = (e_i - e_i)eyh = 0.$$

But $h \leqq g \leqq e$, contradicting maximality.

LEMMA 5.4. *If* $(f_j)_{j \in J}$ *is a family of orthogonal fundamental projections in* A_n, *all having the same order, then* LUB f_j *exists.*

Proof. Repeating the arguments in ([3], Lemme 6.10), we obtain a family (h_α) of orthogonal central projections, with $\mathrm{LUB}\, h_\alpha = 1$, such that, for each α, $J_\alpha = \{j \in J : h_\alpha f_j \neq 0\}$ is finite. For any j, there is an α such that $h_\alpha f_j \neq 0$ (Lemma 1.1), thus $J = \bigcup_\alpha J_\alpha$. For each α, set

$$g_\alpha = \sum_{j \in J_\alpha} h_\alpha f_j = h_\alpha \Big(\sum_{j \in J_\alpha} f_j \Big)$$

(these are finite sums). Since A_n is the C^*-sum of the $h_\alpha A_n$ (Lemma 1.1), there exists a (unique) projection $g \in A_n$ such that $h_\alpha g = g_\alpha$ for all α.

We assert that $g = \mathrm{LUB}\, f_j$. First, given an f_j, let us show $f_j \leqq g$, i.e., $f_j - f_j g = 0$. Given an α, it suffices to show that $(f_j - f_j g)h_\alpha = 0$. If $f_j h_\alpha = 0$, this is clear; if $f_j h_\alpha \neq 0$, then $f_j h_\alpha \leqq g_\alpha$; thus

$$(f_j - f_j g)h_\alpha = (f_j h_\alpha) - (f_j h_\alpha)(h_\alpha g) = (f_j h_\alpha) - (f_j h_\alpha) g_\alpha = 0.$$

Next, if f is a projection such that $f_j \leqq f$ for all j, we must show $g \leqq f$

Fixing α, it suffices to show $(g - gf)h_\alpha = 0$, that is, $g_\alpha = g_\alpha f$. For any j, $h_\alpha f_j \leqq h_\alpha f$; hence $g_\alpha \leqq h_\alpha f$, $g_\alpha = g_\alpha h_\alpha f = g_\alpha f$.

LEMMA 5.5. *If* $(e_i)_{i \in I}$ *is any family of orthogonal projections in* A_n, LUB e_i *exists.*

Proof. By Lemma 5.3, express e_i as the LUB of orthogonal fundamental projections, say $e_i = \mathrm{LUB}\{e_{ij} \colon j \in J_i\}$. Let K denote the set of all ordered pairs (i, j), $i \in I$, $j \in J_i$. For $m = 0, 1, 2, \cdots$, let K_m denote the set of all (i, j) for which e_{ij} has order 2^m. Of course, $K = \bigcup_m K_m$. By Lemma 5.4, we may form $f_m = \mathrm{LUB}\{e_{ij} \colon (i, j) \in K_m\}$. Set $e = \mathrm{LUB}\{f_m \colon m = 0, 1, 2, \cdots\}$ (countable LUB's are legal). We assert that $e = \mathrm{LUB}\, e_i$.

First, given any i, let us show $e_i \leqq e$. If $j \in J_i$, it will suffice to show $e_{ij} \leqq e$. Indeed, if e_{ij} has order 2^m, $e_{ij} \leqq f_m \leqq e$. Finally, supposing g is a projection such that $e_i \leqq g$ for all i, let us show that $e \leqq g$. For all couples $(i, j) \in K_m$, $e_{ij} \leqq e_i \leqq g$; hence $f_m \leqq g$. Varying m, $e \leqq g$.

THEOREM. *If* A *is any* AW^**-algebra, the algebra* A_n *of* $n \times n$ *matrices over* A *is an* AW^**-algebra.*

Proof. According to the discussion in the introduction, we may assume that A is of finite type II. Given any subset $S = \{x_j\}$ of A_n, we must show that the right annihilator of S in A_n is the principal right ideal generated by a projection. The argument for this is given in ([2], Theorem 5.3).

Remarks.

(1) Looking at the scalar subalgebra of A_n, we see that in the passage from A to A_n, type is preserved (although, for homogeneous type I, the order gets multiplied by n).

(2) When A is finite, C_n is, of course, the regular ring of A_n ([1], Section 11).

(3) Let R be any ring with unity, and involution $*$, and let n be a fixed natural number. Let M be the set of all n-ples $x = (x_1, \cdots, x_n)$, $x_i \in R$, provided with the natural left R-module structure. Then R_n identifies with the ring of all module endomorphisms $T \colon M \to M$. Assume further that $x_1 x_1^* + \cdots + x_n x_n^* = 0$ implies $x_1 = \cdots = x_n = 0$. Then $[x, y] = x_1 y_1^* + \cdots + x_n y_n^*$ provides M with an R-valued inner product such that $[x, x] = 0$ implies $x = 0$. If T^* is the "conjugate transpose" of the

matrix T, then $[xT, y] = [x, yT^*]$. For a subset N of M, the orthogonal complement $N^\perp$ is defined in the usual way, and $N \cap N^\perp = 0$.

It is straightforward to verify that the following conditions are equivalent:

(a) the right annihilator of any subset of R_n is the principal right ideal generated by a projection;

(b) for any submodule N of M satisfying $N = N^{\perp\perp}$, one has $M = N + N^\perp$.

Replacing R by an AW^*-algebra A, condition (a) is the assertion that A_n is AW^*. Thus, in this case, condition (b) holds, and we have in effect an n-dimensional non-commutative generalization of ([6], Theorems 3, 7).

STATE UNIVERSITY OF IOWA.

REFERENCES.

[1] S. K. Berberian, "The regular ring of a finite AW^*-algebra," *Annals of Mathematics*, vol. 65 (1957), pp. 224-240.

[2] ———, "On the projection geometry of a finite AW^*-algebra," *Transactions of the American Mathematical Society*, vol. 83 (1956), pp. 493-509.

[3] J. Dixmier, "Les anneaux d'opérateurs de classe finie," *Annales Scientifiques de l'École Normale Supérieure*, vol. 66 (1949), pp. 209-261.

[4] I. Kaplansky, "Projections in Banach alegbras," *Annals of Mathematics*, vol. 53 (1951), pp. 235-249.

[5] ———, "Algebras of type I," *Annals of Mathematics*, vol. 56 (1952), pp. 460-472.

[6] ———, "Modules over operator algebras," *American Journal of Mathematics*, vol. 75 (1953), pp. 839-858.

[7] C. E. Rickart, "Banach algebras with an adjoint operation," *Annals of Mathematics*, vol. 47 (1946), pp. 528-550.

POLARIZED VARIETIES, FIELDS OF MODULI AND GENERALIZED KUMMER VARIETIES OF POLARIZED ABELIAN VARIETIES.*[1]

By T. Matsusaka.

Introduction. In studying theta-functions and abelian functions, we sometimes fix the set of scalar multiples of a principal matrix attached to the given Riemann Matrix. This implies that we fix one divisor class and scalar multiples of it with respect to homology on the corresponding complex torus. In this paper, we shall introduce the corresponding notion in the abstract case, not only to abelian varieties, but also to arbitrary varieties as done in Weil [22]. In fact, on a complete variety V, non-singular in codimension 1, we shall fix one divisor class, with respect to numerical equivalence, and scalar multiples of it (in general V-divisors shall be said to be numerically equivalent to zero if suitable integral multiples are algebraically equivalent to zero on V). Let us call $\mathfrak{X}$ the set of positive V-divisors contained in them. We shall regard V as carrying a structure we get by putting the set $\mathfrak{X}$ on V (cf. Weil [22], pp. 9-10). We shall call such a variety a *polarized variety,* whenever $\mathfrak{X}$ contains a divisor such that the complete linear system determined by it determines an everywhere biregular birational transformation of V into a projective space. First we shall define the set $\mathfrak{X}$ in a somewhat different way, but we shall see later that it is the same as we mentioned. Projective varieties carry *natural* polarizations, which are determined by the sets containing hyperplane sections. The set of varieties, we get by embedding V into projective spaces by means of complete linear systems determined by divisors in $\mathfrak{X}$, is covered by infinitely many algebraic families of varieties. We shall see a relationship between such algebraic families and algebraic families of divisors contained in $\mathfrak{X}$, which is a content of Section 2.

---

* Received October 12, 1956; revised November 11, 1957.

[1] Originally, this work was done while the author was supported by the National Science Foundation through the University of Chicago. After about a year later, the author has moved to the Northwestern University and changed the contents of Section 3 by adding some new results.

We shall follow the same terminology and conventions as in Weil's books (Weil [16], [17]). The writer wishes to express here his thanks to Professor Weil for his valuable advices and criticisms.

In Section 1, we shall state some known results and prove preliminary propositions which we shall need later. In Section 3, we shall prove that the group of everywhere biregular birational transformations of a complete non-singular polarized variety onto itself forms an algebraic group. As a special case, we shall see that the group of automorphisms of a polarized abelian variety is finite. Roughly speaking, the set of everywhere biregular birational transformations of a complete non-singular variety onto itself forms an abstract group, in which one can find the "largest" algebraic group, and to put a structure of polarization on our variety has an effect to cut down the set of cosets, with respect to the algebraic group, to a finite set. In Section 4, we shall prove the existence of the field of moduli of a polarized variety. In the case of elliptic curves, such fields can be generated over the prime field by corresponding j-invariants. In the classical case, when the universal domain is the field of complex numbers, Siegel obtained the result that the field of moduli of a Jacobian variety (polarized by Riemann's theta-divisor in our sense) is the one generated over the complex number field by the corresponding modular functions (cf. Siegel [14]). Finally we shall show the existence of a generalized Kummer variety of a polarized abelian variety over the field of moduli.

Let Z be a positive cycle on an abstract variety U. We shall denote by $|Z|$ the point set attached to Z, i. e. the set of points contained in components of Z. Let U and U' be two varieties with sets of certain structures E and E' respectively. By an *isomorphism* of U with the set of structures E to U' with the set of structures E', we understand an everywhere biregular birational transformation of U to U', mapping E to E'. When $U=U'$, $E=E'$, we say that it is an *automorphism*. We reserve the term "birational transformation" for a general type of transformations with possible fundamental points. When U is a variety defined over a field k, we shall say sometimes that U is *rational* over k.

Let V^n be a complete variety, non-singular in co-dimension 1. We assume that the reader is familiar with linear equivalence and algebraic equivalence of divisors. When two divisors X and X' are linearly equivalent to each other, we write $X \sim X'$. We say that a V-divisor X is *numerically equivalent to* 0 on V if there is a positive integer m such that mX is algebraically equivalent to 0 on V. When V is non-singular, X is usually defined to be numerically equivalent to 0 if and only if $\deg(X \cdot C)=0$ whenever C is a 1-cycle on V such that $X \cdot C$ is defined. When that is so, there is a positive integer m such that mX is algebraically equivalent to 0 on V (cf. Matsusaka [9], Th. 4). Conversely, if mX is algebraically equivalent to 0 on V, we have $\deg(X\cdot C)=0$ whenever C is a 1-cycle on V such that $X\cdot C$ is defined. Therefore the preceding definition of numerical equivalence coincides with the ordinary one when V is non-singular. We denote by $G(V)$, $G_l(V)$, $G_a(V)$ and $G_n(V)$ the group of V-divisors, the group of V-divisors linearly equivalent to 0, the group of V-divisors algebraically equivalent to 0 and the group of V-divisors numerically equivalent to 0 respectively. It is known and easy to see that $G(V)\supset G_n(V)\supset G_a(V)\supset G_l(V)$. We denote by $\mathfrak{L}^*$, $\mathfrak{A}^*$, and $\mathfrak{N}^*$ cosets (divisor classes) of $G(V)$ mod $G_l(V)$, mod $G_a(V)$ and mod $G_n(V)$ and by $\mathfrak{L}$, $\mathfrak{A}$, and $\mathfrak{N}$ the sets of positive divisors contained in $\mathfrak{L}^*$, $\mathfrak{A}^*$ and $\mathfrak{N}^*$. $\mathfrak{L}^*$, $\mathfrak{A}^*$ or $\mathfrak{N}^*$ (resp. $\mathfrak{L}$, $\mathfrak{A}$ or $\mathfrak{N}$) is determined uniquely by one of divisors contained in it. When $\mathfrak{L}^*$, $\mathfrak{A}^*$ or $\mathfrak{N}^*$ (resp. $\mathfrak{L}$, $\mathfrak{A}$ or $\mathfrak{N}$) contains a divisor Z, we denote it sometimes by $\mathfrak{L}^*(Z)$, $\mathfrak{A}^*(Z)$ or $\mathfrak{N}^*(Z)$ (resp. $\mathfrak{L}(Z)$, $\mathfrak{A}(Z)$ or $\mathfrak{N}(Z)$). Let m be a positive integer, then we denote by $m\mathfrak{A}^*$, for instance, the divisor class mod $G_a(V)$ determined by a divisor mY with Y in $\mathfrak{A}^*$. We denote by $m\mathfrak{A}$ the set of positive divisors in $m\mathfrak{A}^*$. We do the same for $\mathfrak{L}^*$, $\mathfrak{L}$ and $\mathfrak{N}^*$, $\mathfrak{N}$.

We can define *specializations of cycles* on abstract varieties. Specializations are compatible with the operations of addition, multiplication and algebraic projection. As far as positive cycles are concerned, specializations are compatible with the operation of intersection-product. Moreover, when the ambient variety is complete and non-singular in co-dimension 1, linear equivalence, algebraic equivalence and numerical equivalence of divisors are preserved by specializations. For the general treatment of specializations of cycles, we refer to the paper by G. Shimura (cf. Shimura [13]). We write $X\rightarrow X'$ ref. k, if a cycle X' is a specialization of X over a field k.

Let Z be a positive divisor on a product $W\times V$, k be a common field of definition for W and V over which Z is rational and w be a generic point of W over k. Let $\mathfrak{F}$ be the set of V-divisors which are specializations of $Z(w)$ over k. $\mathfrak{F}$ is usually known as an *algebraic family of positive divisors* on V and (W,Z) is called a *parametrization* of $\mathfrak{F}$ over k. We call $Z(w)$ a generic divisor of $\mathfrak{F}$ over k. When there is a parametrization of $\mathfrak{F}$ over a field k' containing a field of definition of V, we say that $\mathfrak{F}$ is defined over k'. It is known that $\mathfrak{L}$ is an algebraic family of positive divisors (cf. Matsusaka [5], Lemma 4) and is called sometimes a *complete linear system.* The set of rational functions f on V such that $(f)\succ -Z$ forms a module $L(Z)$ and we denote by $l(Z)$ the dimension of the module. $l(Z)-1$ is known as the (geometric) dimension of our complete linear system $\mathfrak{L}(Z)$. In general, let $\mathfrak{M}$ be a finitely generated module of rational functions on V over the universal domain and let $(f_0,\cdots,f_r)$ be a basis of $\mathfrak{M}$. Let k be a common field of definition for V and for every f_i and let $(u_0, \cdots, u_r)$ be a set of independent variables over k. The set of divisors of the form $(\sum c_if_i) + (\sum u_if_i)_\infty$ forms an algebraic family contained in $\mathfrak{L}((\sum u_if_i)_\infty)$ and it is called a *linear system* or the *linear system determined by* $\mathfrak{M}$. Let x be a generic point of V over k, then we can define a rational mapping of V into an affine space or a projective space by $x \to (f_0(x), \cdots, f_r(x))$. We say that such a mapping is a *rational mapping determined by* $\mathfrak{M}$ or *determined by the corresponding linear system.* We say that it is *non-degenerate,* since $f_0, \cdots, f_r$ are linearly indepenedent. When $\mathfrak{M}$ is the module $\mathfrak{L}(Z)$ itself, we say that it is a rational mapping *determined by Z.* In particular, when the rational mapping is an isomorphism of V into a projective space, we say that it is a non-degenerate *projective embedding* of V. We say that the linear system corresponding to $\mathfrak{M}$ is *ample* if it has no fixed component and determines a non-degenerate projective embedding of V. If a V-divisor X is such that the linear system $\mathfrak{L}(X)$ is ample, we say that X is *linearly effective.* We say that X is *algebraically* (resp. *numerically*) *effective,* when every divisor in $\mathfrak{A}(X)$ (resp. $\mathfrak{N}(X)$) is linearly effective.

Let $\mathfrak{F}$ be an algebraic family of positive V-divisors. We say that $\mathfrak{F}$ is *maximal,* when there is no algebraic family of divisors on V containing $\mathfrak{F}$. We say that $\mathfrak{F}$ is *quasi-complete* when the set $\mathfrak{A}$ containing $\mathfrak{F}$ coincides with $\mathfrak{F}$. We say that $\mathfrak{F}$ is complete if it is quasi-complete and every divisor in it determines a complete linear system of the same dimension. There is an algebraic family $\mathfrak{F}$ of positive V-divisors with the following property: When Z is in $G_a(V)$, there is a divisor X in $\mathfrak{F}$ such that $Z \sim X - X_0$ with a fixed X_0 in $\mathfrak{F}$ (cf. Matsusaka [5], Th. 1). Such a family is called a *total family.* Chow and v. d. Waerden proved, by means of Chow-forms, that $\mathfrak{N}$ is a union of a finite set of maximal algebraic families of positive V-divisors (cf. Chow-v. d. Waerden [4]). Let X be now a positive cycle on a projective space. Then the set of coefficients of the Chow-form of X may be regarded as a set of homogeneous coordinates of a point in a projective space, which we call the *Chow-point* of X. When X is on a product of projective spaces, there is the standard isomorphism of such a product into a projective space, and by means of it we can identify X with a cycle on a projective space. By the Chow-point of such X, we understand the Chow-point of the transformed cycle by the isomorphism.

Finally, let us recall some of the known results on Picard varieties which we need later. Let, as before, V be a complete algebraic variety, non-singular in co-dimension 1 and K be a field of definition for V. Let f be a mapping of $G_a(V)$ into an algebraic variety W with the following properties: (i) f is well-defined outside of a proper subset of $G_a(V)$; (ii) there is a common field of definition K' for V and W such that whenever Z is in $G_a(V)$ and rational over a field K'' containing K', $f(Z)$ is rational over Z'' if it is defined; (iii) when $Z, Z' \in G_a(V)$, $Z \rightarrow Z'$ ref. K' and when f is defined at Z and Z', then $f(Z) \rightarrow f(Z')$ ref. K'. If f satisfies the above conditions, we say that f is a *rational mapping* of $G_a(V)$ and that K' is a *field of definition* for f. Moreover, when W is a group variety and f is also a group homomorphism, we say that f is a *rational homomorphism*. There is an abelian variety P and a rational homomorphism f of $G_a(V)$ onto P such that the kernel of f is $G_l(V)$ and that f has the universal mapping property as a rational homomorphism of $G_a(V)$ into an abelian variety. P is called the *Picard variety* of V and f the *canonical rational homomorphism* of $G_a(V)$ onto P. For these, see Chow [3], Matsusaka [5], [6] and Néron-Samuel [11].

Section 1.

1. Let us summarize here some of the known results, which we shall need later in this paper.

THEOREM 1. *Let V be a non-singular variety in a projective space. (i) $G_n(V)/G_a(V)$ is a finite group. (ii) When X is a linearly effective V-divisor and Y is an arbitrary V-divisor, there is a positive integer m_0 with the following properties: Whenever a positive integer m is such that $m > m_0$, $Y + mX$ is numerically effective and $\mathfrak{R}(Y + mX)$ consists of a finite set of complete total families $\mathfrak{A}_1, \cdots, \mathfrak{A}_t$, where t is the order of $G_n(V)/G_a(V)$.*

As to these, see Matsusaka [9], Th. 4 and [7], Th. 2 (cf. also the proof of Matsusaka [7], Lemma 2. There it is proved that $Y + mX$ is linearly effective when m is sufficiently large).

Let A be an abelian variety and X be a divisor on A. We say that X is *non-degenerate* if the set of points a on A such that $X_a \sim X$ is finite. It is easy to see that on every abelian variety there is at least one non-degenerate positive divisor. On a simple abelian variety, every positive divisor is non-degenerate and the existence of such divisors on a general abelian variety can be seen by decomposing it into a product of simple abelian varieties in the sense of isogeny (Weil [17], Th. 28).

THEOREM 2. *Let X be a positive non-degenerate divisor on an abelian variety. There is a positive integer m_0 such that whenever $m > m_0$, mX is linearly effective.* (Cf. Weil [19]).

2.

PROPOSITION 1. *Let A be an abelian variety and $\mathfrak{F}$ be a maximal algebraic family of positive A-divisors. Let X be a divisor in $\mathfrak{F}$, then any divisor X' in $\mathfrak{F}$ is such that $X' \sim X_u$.*

Proof. Let $P(A)$ be the Picard variety of A, f be the canonical homomorphism of $G_a(A)$ onto $P(A)$ and k be a common field of definition for $A, \mathfrak{F}, P(A)$ and for f. Let Y be a generic divisor of $\mathfrak{F}$ over k, then the rational mapping f_Y defined by $f_Y(u) = f(Y_u - Y)$ into $P(A)$ is a homomorphism of A into $P(A)$. Since Y is rational over a regular extension of k, f_Y is defined over a regular extension of k, which implies that f_Y is defined over k by a result of Chow (cf. Chow [2]). Let O be the neutral element of $P(A)$, and let C be the connected component of the algebraic group $|f_Y^{-1}(O)|$ containing the neutral element of A. C is defined over the algebraic closure of k and since $Y_u \sim Y$ whenever u is a point of C, it follows that $X_u \sim X$ for any point u on C ($\sim$ is preserved by specializations!).

There is an abelian subvariety B of A and a homomorphism α from $C \times B$ onto A such that $\alpha(u,v) = u + v$, $B \cap C$ is a finite group and that the kernel of α is a finite group (Weil [17], Prop. 25, Th. 26). We may obviously assume that B, C and α are all defined over k, replacing k by its algebraic closure, if necessary. Put $U = \alpha^{-1}(Y)$, $W = \alpha^{-1}(X)$. Let further $O, d_1, \cdots, d_m$ be all the distinct points in the kernel of α. U and W are obviously invariant by translations T_{d_i}. Let u be a point on A and v be one of the points on $C \times B$ such that $\alpha(v) = u$. Let T be the graph of α. Applying the translation $T_{v,u}$ to $T \cdot (C \times B \times Y)$ on $C \times B \times A$, we get $\alpha^{-1}(Y_u) = U_v$. In the same way, $\alpha^{-1}(X_u) = W_v$. When u is a point on C, denoting by O' the neutral element of B, (u, O') is one of the points on $C \times B$ which are mapped to u by α. Therefore $U_{(u,O')} \sim U$ for any u on C. We claim that U has the projection C on C. Suppose the contrary, then U is of the form $Z \times B$ and $Z_u \sim Z$ for every u on C. This implies that Z is numerically equivalent to zero and since U is positive, it is impossible (cf. Weil [18], p. 123).

Let t and t' be two independent generic points of C over k. We have $U_{(t,O')}(t') \sim U(t')$, and the former is nothing but $U(t'-t)$. Therefore, since t and $t'-t$ are again independent generic points of C over k, we see that $U(t) \sim U(t')$ for any pair of points (t,t') whenever they are defined. This implies that $U \sim C \times M + N \times B$ where M and N are B- and C-divisors respectively. We have $N_t \sim N$ for any t on C and since $U \succ 0$, we see that $U \sim C \times M$. Let b be a point on B such that $M_b \sim M$. Then $U_{(O'',b)} \sim U$

where O'' is the neutral element of C, and this implies that $sY_b \sim sY$ for a certain positive integer s (Weil [16], Chap. VIII, Th. 7). Hence $Y_{sb} \sim Y$ by Weil [17], Cor. 2, Th. 30. When that is so, sb is contained in $|f_Y^{-1}(O)|$, and since B and $|f_Y^{-1}(O)|$ have only a finite set of points in common, such sb and hence b must form a finite set (cf. Weil [17], Cor. 1, Th. 33). This proves that M is a non-degenerate divisor on B. In the same way, $W \sim C \times M'$, where M' is a B-divisor. Since U and W are algebraically equivalent to each other, so are M and M'. Moreover, since M is non-degenerate, there is a point w on B such that $M \sim M'_w$ and consequently $W_{(O'',w)} \sim U$, because B and its Picard variety have the same dimension (Chow [3], Matsusaka [8]). Going back to A, we see that $sY_w \sim sX$.

Let K be a field containing k over which X is rational and let Y be now a generic divisor of $\mathfrak{F}$ over K. Since $f(Y - X)$ is rational over a regular extension of K, it has a locus E over K on $P(A)$. Let x be a point on A, then since $f(X_x - X)$ is rational $K(x)$, it has a locus E' over K on $P(A)$. The endomorphism $s\delta$ on $P(A)$ is surjective (Weil [17], Cor. 1, Th. 33) and E, E' are mapped onto themselves by the endomorphism. But the relation $sY_w \sim sX$ asserts that the image of E by the endomorphism is contained in E', which proves that $E \subset E'$. Our proposition is thereby proved.

PROPOSITION 2. *Let A be an abelian variety and X be a divisor on A, which we assume to be positive. When X is linearly effective, X is non-degenerate, algebraically effective and $\mathfrak{A}(X)$ forms a complete total family. When $\mathfrak{A}(X)$ contains a total family, X is non-degenerate and $\mathfrak{A}(X)$ is a complete total family.*

Proof. By our definition, when X is linearly effective, we may assume that A is a projective variety and that X is a hyperplane section of A. There is a positive integer m such that $\mathfrak{A}(mX)$ is a complete total family by Th. 1, (ii). If we can show that mX is non-degenerate, then we see immediately that X is non-degenerate by Weil [17], Cor. 2, Th. 30. When that is so, $\mathfrak{A}(X)$ must be a complete total family and every divisor in $\mathfrak{A}(X)$ is linearly equivalent to a translation of X since A and its Picard variety have the same dimension. Moreover when that is so, every divisor in $\mathfrak{A}(X)$ is linearly effective. Therefore, in order to prove our proposition, it is sufficient to prove the following: When $\mathfrak{A}(X)$ contains a maximal total family $\mathfrak{F}$ of divisors, X is non-degenerate.

Let X' be a fixed divisor in $\mathfrak{F}$, then by our Prop. 1, when Y is a divisor in $\mathfrak{F}$, there is a point v on A such that $Y \sim X'_v$. Let $P(A)$ be the Picard variety of A and f be the canonical mapping of $G_a(A)$ onto $P(A)$. Since

$\mathfrak{F}$ is total, any point on $P(A)$ can be written as $f(Y-X')$ with some Y in $\mathfrak{F}$. Therefore, any point on $P(A)$ can be written as $f(X'_v-X')$ with some v on A. Since A and $P(A)$ have the same dimension, it follows now that the set of points u on A with $X'_u \sim X'$ is finite, hence that X' is a non-degenerate divisor. Since $X \sim X'_a$ for some a on A, X is also non-degenerate and our proposition is thereby proved.

Section 2.

3. Let V be a complete variety, non-singular in co-dimension 1, and let X be a positive V-divisor. Let $\mathfrak{X}$ be the set of positive divisors X such that $mX \equiv m'X_0 \bmod G_a(V)$ for a pair (m, m') of positive integers. $\mathfrak{X}$ is uniquely determined when one of the divisors contained in it is given. $\mathfrak{X}$ defines a *structure* on V and when $\mathfrak{X}$ contains a linearly effective divisor, we shall call it a *structure of polarization* (cf. Bourbaki [1], § 8). Any divisor in $\mathfrak{X}$ is called a *polar divisor*. When we regard V as a variety with a structure of polarization, we shall say that V is a *polarized variety* polarized by $\mathfrak{X}$. We shall say that a polarized variety V, polarized by $\mathfrak{X}$, is *defined* over a field k, when V is defined over k and $\mathfrak{X}$ contains a rational divisor over k. For these definitions, see also Weil [22].

When A is an abelian variety, we remark here that it is a variety with an additional structure which we get by putting a point on it (this means that we fix on A one definite law of composition, since the law of composition on A can be determined uniquely up to translations).

Let V be an ordinary variety, E', E'' be two sets of structures and V' (resp. V'') be the variety which we get from V by putting the set of structures E' (resp. E'') on V. When $E' \subset E''$, we say that V' is the *underlying variety* of V'' with the set of structures E'. For instance, the underlying polarized variety of a polarized abelian variety A is the polarized variety which we get from A by removing the structure of the group.

From now on, let us assume that the underlying varieties are non-singular varieties unless the contrary is specifically stated. We can define a *natural* polarization on any projective variety, that is, the polarization defined by the set $\mathfrak{X}$ determined by a hyperplane section of it. Hereafter, let us assume that "a polarized projective variety" means a non-singular projective variety polarized by its natural polarization unless the contrary is specifically stated. Let V be a polarized variety, polarized by a set $\mathfrak{X}$. Let X be a linearly effective divisor in it. The complete linear system $\mathfrak{L}(X)$ defines a non-degenerate projective embedding f_X of V, which is determined uniquely up to projective transformations by $\mathfrak{L}(X)$. Let us assume that V has a set of structures E;

we denote by $f_X(V)$ the transform of V with the set of structures $f_X(E)$. Let $\mathfrak{S}$ be a subset of $\mathfrak{X}$. We shall denote by $\mathfrak{P}(V, \mathfrak{S})$ the set of transforms $f_X(V)$, where the f_X are non-degenerate projective embeddings of V determined by linearly effective divisors X in $\mathfrak{S}$.

4.

Lemma 1. *Let T be a projective transformation in a projective space defined over a field k and let T^* be a projective transformation in the same space defined by a matrix whose elements are independent variables over k. Then T is a specialization of T^* over k.*

Since the proof is easy, we shall omit it. Such a projective transformation as T^* shall be called a "generic projective transformation" over k.

Proposition 3. *Let W be a variety in a projective space L^n and let $\mathfrak{S}$ be the set of varieties in L which are projectively equivalent to W. Let G be the group variety $PGL(n)$. There is a subvariety X of $G \times W \times L$ such that $(t' \times W \times L) \cdot X$ is defined for every point t' on G, that* $\mathrm{pr}_3((t' \times W \times L) \cdot X)$ *is in $\mathfrak{S}$ and that every variety in $\mathfrak{S}$ can be obtained in this way.*

Proof. G is a non-singular variety defined over the prime field with its law of composition. Let k be a field of definition for W, t and u be independent generic points of G and L over k. Let T_t be the projective transformation corresponding to t. Let X^* be the locus of $(t, u, T_t(u))$ over k. X^* is a subvariety of $G \times L \times L$ and the projection of X^* on $G \times L$, where L may be any one of the last two factors of $G \times L \times L$, is everywhere regular. Therefore $X^* \cdot (G \times W \times L)$ is defined, is a variety and it is the unique subvariety of X^* lying over $G \times W$ by Weil [16], Chap. IV, Th. 15.

Let t' be a point on G and consider the intersection $(t' \times W \times L) \cap X$ on $G \times W \times L$, where $X = X^* \cdot (G \times W \times L)$. Since the projection of X on $G \times W$ is everywhere regular, the intersection reduces to a variety and it is the uniquely determined subvariety of X having the projection $t' \times W$ on $G \times W$ by the same theorem of Weil. Hence $(t' \times W \times L) \cdot X$ is defined and is of the form $t' \times W_{t'}$, where $W_{t'}$ is the variety having the same dimension as W. We can see easily that $W_{t'}$ is the graph of the restriction of $T_{t'}$ on $W \times T_{t'}(W)$ and so $\mathrm{pr}_3((t' \times W \times L) \cdot X) \in \mathfrak{S}$.

Conversely, let W'' be a variety in $\mathfrak{S}$, then there is a point t'' on G such that $W'' = T_{t''}(W)$. By what we have already observed, $W_{t''}$ is the graph of the restriction of $T_{t''}$ on $W \times T_{t''}(W)$ and therefore

$$W'' = \mathrm{pr}_3((t'' \times W \times L) \cdot X).$$

COROLLARY. *Notations being the same as the preceding proposition, let k be a common field of definition for G and W. Let t be a generic point of G over k and x be the Chow-point of $T_t(W)$. x has a locus U over k, which is independent of a choice of a generic point t and also of a choice of a variety W from $\mathfrak{S}$. There is a rational mapping g_W of G onto U when W is fixed in $\mathfrak{S}$ and it has the following properties:*

(i) *g_W is everywhere defined;*

(ii) *$g_W(t')$ is the Chow-point of $T_{t'}(W)$ whenever t' is a point of G;*

(iii) *The set-theoretic image of G by g_W is an open subset of U;*

(iv) *g_W is defined over k.*

Proof. T_t is defined over $k(t)$ which is a regular extension of k and clearly $T_t(W)$ is defined over the same field. Therefore, the Chow-point of $T_t(W)$ is rational over $k(t)$, which implies that x has a locus U over k. Now let W' be another variety in $\mathfrak{S}$. There is a projective transformation T such that $T(W') = W$. Hence $\mathfrak{S}$ is the set of varieties projectively equivalent to W'. Since U is the closure of the set of Chow-points of varieties in $\mathfrak{S}$, U is independent of a choice of W from $\mathfrak{S}$. Since $k(x)$ is a subfield of $k(t)$, there is a rational mapping $g_W = g$ from G onto U such that $g(t) = x$. Let t' be any point on G. By Proposition 3, $\mathrm{pr}_3((t' \times W \times L) \cdot X)$ is defined and consequently x has the uniquely determined specialization over $t \rightarrow t'$ ref. k. Therefore g is single-valued at t' and since G is non-singular, it follows that g is defined at t'. Of course $g(t')$ is the Chow-point of $T_{t'}(W)$. Thus, except for (iii), everything is proved.

It is easy to see that U is a pre-homogeneous space on which G is acting, and G acts transitively on the set-theoretic image U' of G by g. Moreover, since it consists of Chow-points of varieties in $\mathfrak{S}$, G cannot transform any point in U' to a point of $U - U'$. This means that U' is the largest subset of U which is biregularly equivalent to the homogeneous space birationally equivalent to the pre-homogeneous space U. Hence U' must be an open set on U (as to pre-homogeneous and homogeneous spaces, see Weil [20]).

5. We can say, by virtue of the corollary to our Proposition 3, that the set of varieties projectively equivalent to a variety in a projective space forms an algebraic family, since we can identify the set with an open algebraic variety. We are going to prove the same for $\mathfrak{P}(V, \mathfrak{A})$, where $\mathfrak{A}$ is a complete algebraic family of divisors on V consisting of algebraically effective divisors. Here we shall prove some preliminary lemmas which we shall need for the purpose.

LEMMA 2. *Let W be a normal variety in a projective space and X, Y be two positive W-divisors. Let k be an algebraically closed field of definition for W and assume that $X \rightarrow Y$ ref. k and that $l(X) = l(Y)$. Let g be a non-degenerate rational mapping of W into a projective space determined by $\mathfrak{L}(Y)$, then there is a non-degenerate rational mapping f of W into a projective space such that $(X, f) \rightarrow (Y, g)$ ref. k, when $\mathfrak{L}(Y)$ has no base point.*

Proof. Let $r+1$ be the common value of $l(X)$ and $l(Y)$ and U, U' be the Chow-varieties of $\mathfrak{L}(X)$, $\mathfrak{L}(Y)$. Since linear equivalence is preserved by specializations and since U and U' have the same dimension, it follows that $(X, |U|) \rightarrow (Y, |U'|)$ ref. k. Replacing k by a bigger field and replacing X by a generic specialization of it over k, if necessary, we may assume that Y, g are rational over k. Then U' is a variety defined over k (Matsusaka [5], Lemma 1). Let $Y_0, \cdots, Y_r$ be divisors in $\mathfrak{L}(Y)$ corresponding to $r+1$ independent generic points $y_0, \cdots, y_r$ of U' over k. There is a set of divisors $(X_0, \cdots, X_r)$ in $\mathfrak{L}(X)$ corresponding to a set of $r+1$ independent generic points $x_0, \cdots, x_r$ of U over a defining field K of U containing k such that

$$(X, |U|, X_0, \cdots, X_r) \rightarrow (Y, |U'|, Y_0, \cdots, Y_r) \text{ ref. } k.$$

Since $\mathfrak{L}(Y)$ has no base point, it is easy to see that there is no base point for $\mathfrak{L}(X)$. By our choice of $(X_0, \cdots, X_r)$ and $(Y_0, \cdots, Y_r)$, it follows that sets of functions $(1, h_1, \cdots, h_r)$ and $(1, h'_1, \cdots, h'_r)$ defined by $(h_i) = X_i - X_0$, $(h'_i) = Y_i - Y_0$ form bases of $L(X_0)$ and $L(Y_0)$ respectively. Since $(x) \rightarrow (y)$ ref. k, there is a field k' containing k, a generic specialization (x^*) of (x) over k and two sets (z^*), (z') of quantities such that (x^*, z^*) has a locus C of dimension 1 over k' on which (y, z') is a simple rational point over k' (Weil [16], Appendix II, Prop. 7). Replacing everything related to X by a generic specialization of it over k, we may assume that $k' = k$ and we shall omit *. Let us denote the points (x, z) and (y, z') by Q and Q'. Since every X_i is rational over $k(Q)$, we may assume that h_i is defined over $k(Q)$ (Weil [16], Chap. VIII, Cor. 1, Th. 10). Let w be a generic point of W over $k(Q, Q')$. There is a function H_i on $C \times W$ with a field of definition k such that $H_i(Q, w) = h_i(w)$. By multiplying a suitable constant from $k(Q)$ to h_i, we may assume that $Q' \times W$ is not a component of (H_i) for every i. Then $(H_i) \cdot (Q' \times W)$ is defined. We have $(Q \times W) \cdot (H_i)_0 = Q \times X_i$ and $(Q \times W) \cdot (H_i)_\infty = Q \times X_0$ (Weil [16], Chap. VIII, Cor. 1, Th. 4). By the compatibility of specializations with the operation of intersection product, we see that $(Q' \times W) \cdot (H_i)_0 = Q' \times Y_i$ and $(Q' \times W) \cdot (H_i)_\infty = Q' \times Y_0$.

Let f be the rational mapping of W into a projective space defined by $w \rightarrow (1, h_1(w), \cdots, h_r(w))$ and g' be the rational mapping of W into the same projective space defined by $w \rightarrow (1, h'_1(w), \cdots, h'_r(w))$. Let $T_f, T_g, T_{g'}$ be graphs of f, g, g' and $(Q, T_f) \rightarrow (Q', T')$ ref. k be an extension of $Q \rightarrow Q'$ ref. k. Since k is algebraically closed, we may take as T' one which is rational over k. H_i is defined at (Q', w), the function h^*_i defined by $H_i(Q', w) = h^*_i(w)$ is defined over k and is such that $(h^*_i) = Y_i - Y_0$. Hence h^*_i and h'_i differ by a constant from k and we may assume that they are actually the same. Let (w', v') be a point on a component of T'. There is a point w^* of W such that $(Q, T_f, w^*, T_f(w^*)) \rightarrow (Q', T', w', v')$ ref. k. Assume first that w' is not in $|Y_0|$. Then H_i is defined at (Q', w') and $H_i(Q', w')$ is the uniquely determined specialization of $H_i(Q, w^*)$ over $(Q, w^*) \rightarrow (Q', w')$ ref. k. Therefore $(1, H_1(Q', w'), \cdots, H_r(Q', w'))$ must be a representative of v', which is the same as $(1, h'_1(w'), \cdots, h'_r(w'))$. Hence (w', v') must be a point on $T_{g'}$. When w' is on $|Y_0|$, let us choose an index j so that $|Y_j|$ does not contain w' and take H_i/H_j for H_i. Then the same arguments show that (w', v') is on $T_{g'}$. Therefore in any case $|T'|$ must be contained in $|T_{g'}|$ as a point set. Moreover since both have the same dimension and since $T_{g'}$ is a variety, we see that T' must be an integral multiple of $T_{g'}$. By the compatibility of specializations with the operation of algebraic projection, we finally get $T' = T_{g'}$. g and g' differ by a projective transformation F defined over k since k is algebraically closed. Let F^* be a generic projective transformation over a common field of definition for W, C, Q, Q', T_f, T_g and $T_{g'}$ containing k, then $(Q, f, F^*) \rightarrow (Q', g', F)$ ref. k. Since F and F^* are isomorphisms, $F \cdot g'$ is the uniquely determined specialization of $F^* \cdot f$ over that specialization with reference to k. Since $F^* \cdot f$ is also a non-degenerate rational mapping of W into the projective space determined by $\mathfrak{L}(X)$, our lemma is proved.

LEMMA 3. *Let* U_i $(i = 1, 2, 3)$ *be three varieties and* X *and* Y *be simple subvarieties of* $U_1 \times U_2$ *and* $U_2 \times U_3$ *respectively. Assume that the projection of* Y *on* U_2 *is* U_2 *and is regular at every point of* U_2. *Then* $(X \times U_3) \cdot (U_1 \times Y)$ *is defined on* $U_1 \times U_2 \times U_3$ *and is a cycle of the form* $1 \cdot Z$ *where* Z *is a subvariety of* $U_1 \times U \times U_3$, *which is the only component of* $X \times U_3 \cap U_1 \times Y$. *When* Y *is an isomorphism,* $\mathrm{pr}_{13}((X \times U_3) \cdot (U_1 \times Y)) = Y \circ X$ *is not* 0 *and* $\mathrm{pr}_{13}((X \times U_3) \cdot (U_1 \times Y)) = \mathrm{pr}_{13}((X' \times U_3) \cdot (U_1 \times Y))$ *implies* $X = X'$ *for any cycle* X' *on* $U_1 \times U_2$; *and if* $\mathrm{pr}_{13}((X \times U_3) \cdot (U_1 \times Y))$ *is a birational correspondence (resp. isomorphism), then* X *is a birational correspondence (resp. isomorphism).*

Proof. Let k be an algebraically closed common field of definition for the U_i, X and Y and for every component of X'. Let f be the rational mapping of U_2 into U_3 with the graph of Y and (x,y) be a generic point of X over k. $(y,f(y))$ is a generic point of Y over k. Let (x',y',z') be any point in $X \times U_3 \cap U_1 \times Y$. (x',y') is then a point on X and (y',z') is a point on Y, and consequently $z'=f(y')$. This shows that the above intersection reduces to the subvariety Z which is the locus of $(x,y,f(y))$ over k. Since x,y and $f(y)$ are simple on U_1, U_2 and U_3 respectively, Z is a simple subvariety of $U_1 \times U_2 \times U_3$. This proves that $(X \times U_3) \cdot (U_1 \times Y) = mZ$ with a positive integer m.

Assume that Y is an isomorphism. Then $k(x,y,f(y))$ is the same as $k(x,f(y))$ and hence the projection Z' of Z on the product $U_1 \times U_3$ has the same dimension as Z and the projection of Z on $U_1 \times U_3$ is regular. Assume that Z' is a birational correspondence. Then $k(x)=k(f(y))=k(y)$ and this shows that X is a birational correspondence. When Z' is an isomorphism, it is easy to see that X is an isomorphism.

Returning to the general case, we have to prove $m=1$, and in order to do so, we may assume that every U_i is an affine variety. Let H be a generic hyperplane over k in the ambient affine space of U_1 and (u) be the set of coefficients of the defining equation for H. $H \cdot U_1$ is defined and the intersection-product $(H \cdot U_1 \times U_2 \times U_3) \cdot (X \times U_3)$ is also defined on $U_1 \times U_2 \times U_3$ (Weil [16], Chap. V, Prop. 14), which can be written as $(H \cdot U_1 \times U_2) \cdot X \times U_3$ (cf. Weil [16], Chap. VII, Th. 11) and is prime rational over $k(u)$. Since $(X \times U_3) \cdot (U_1 \times Y)$ and $(X \times U_3) \cdot (H \cdot U_1 \times U_2 \times U_3)$ are defined and since $X \times U_3$, $U_1 \times Y$ and $H \cdot U_1 \times U_2 \times U_3$ intersect properly on $U_1 \times U_2 \times U_3$, we see that

$$((U_1 \times Y) \cdot (X \times U_3)) \cdot (H \cdot U_1 \times U_2 \times U_3) = (U_1 \times Y) \cdot ((H \cdot U_1 \times U_2) \cdot (X \times U_3))$$

by Weil [16], Chap. VII, Th. 10. Moreover, since the projection of $U_1 \times Y$ on $U_1 \times U_2$ is defined everywhere, it follows that

$$(U_1 \times Y) \cdot ((H \cdot U_1 \times U_2) \cdot (X \times U_3))$$

is prime rational over $k(u)$ (Weil [16], Chap. VI, Th. 8), which can also be written as $mZ \cdot (H \cdot U_1 \times U_2 \times U_3)$. Since $Z \cdot (H \cdot U_1 \times U_2 \times U_3)$ is rational over $k(u)$, m must be 1. Hence our assertion about m is proved. The rest of our assertions follow immediately.

6.

LEMMA 4. *Let U be a complete normal variety, and $\mathfrak{A}$ be a complete algebraic family of U-divisors consisting of algebraically effective positive divisors. Let K be a common field of definition for U and $\mathfrak{A}$. Let V be the set of Chow-points of non-degenerate projective embeddings of U determined by divisors in $\mathfrak{A}$, then V is an open algebraic variety in a projective space defined over a field K.*

Proof. Let $\bar{K}$ be the algebraic closure of K and X be a generic divisor of $\mathfrak{A}$ over K. By Lemma 2, the set of Chow-points of non-degenerate projective embeddings determined by divisors in $\mathfrak{A}$, together with their specializations over $\bar{K}$, forms an algebraic variety V' defined over $\bar{K}$. Let v be a generic point of V' over $\bar{K}$, then it is the Chow-point of a non-degenerate projective embedding of U determined by a generic divisor of $\mathfrak{A}$ over K, which we may identify with X. Let f_X be the projective embedding, and T be the graph of it. There is a closed set $\mathfrak{F}$ over $\bar{K}$ on V' such that a specialization T' of T over $\bar{K}$ is irreducible if and only if the Chow-point of T' is in $V'-\mathfrak{F}$; denoting by L^* the ambient space of $f_X(U)$, and denoting by L a hyperplane in L^*, there is a closed subset $\mathfrak{F}'$ over $\bar{K}$ on V' such that T' is not contained in any $U \times L$ if and only if the Chow-point of T' is in $V'-\mathfrak{F}'$ (cf. Chow-v. d. Waerden [4]; v. d. Waerden [15]).

Let again T' be a specialization of T over $\bar{K}$, and now assume that its Chow-point is in $V'-\mathfrak{F}-\mathfrak{F}'=V$. Since T' is irreducible and $\mathrm{pr}_U T'=U$ by the compatibility of specializations with the operation of algebraic projection, T' is the graph of a rational mapping f' of U into L^*. We claim that f' is a non-degenerate projective embedding of U determined by a divisor in $\mathfrak{A}$. Let L be an arbitrary hyperplane in L^* and assume that the Chow-point of T is a generic point of V over a field K' containing $\bar{K}$ over which L is defined. Then we have $((U\times L)\cdot T, T) \rightarrow ((U \times L)\cdot T', T')$ ref. K', and since we have $X \sim \mathrm{pr}_U((U\times L)\cdot T)$, it follows that $\mathrm{pr}_U((U\times L)\cdot T') \in \mathfrak{A}$. Let x be a generic point of U over K', (y) be a representative of $f'(x)$ and put $y_i = g_i(x)$ $(i=0, 1, \cdots, N=\dim L^*)$. Since $(U\times L)\cdot T'$ is defined for all L, it follows that $g_0, \cdots, g_N$ are linearly independent. Since $\mathfrak{A}$ is complete, we have $l(X)=l(\mathrm{pr}_U((U\times L)\cdot T'))$ and this shows that f' is a non-degenerate projective embedding determined by a divisor in $\mathfrak{A}$. Now conversely, if T' is the graph of a non-degenerate projective embedding of U determined by a divisor in $\mathfrak{A}$, the Chow-point of it must be on V' by Lemma 2 and it must not be contained in $\mathfrak{F}$ and in $\mathfrak{F}'$. Our lemma will be proved if we show that V is defined over K.

Since X is a generic divisor of $\mathfrak{A}$ over K, X is rational over a regular extension K^* of K. Since X is rational over K^*, we can find a set of functions $h_0, \cdots, h_N$, all defined over K^*, which forms a basis of $L(X)$ (cf. Weil [16], Th. 10). Hence there is a non-degenerate projective embedding f determined by X defined over K^*. Since any other such embedding can be written as $F \cdot f$, where F is a projective transformation of L^*, it follows that there is a non-degenerate projective embedding f^* determined by X such that it is defined over a regular extension of K and that any other non-degenerate projective embedding determined by a divisor in $\mathfrak{A}$ is a specialization of f^* over $\bar{K}$ by our Lemmas 1, 2. This proves that V' is defined over K. Then it immediately follows that $\mathfrak{H}$ and $\mathfrak{H}'$ are closed subsets of V' over K. Our lemma is thereby proved.

LEMMA 5. *Let V be a variety in a projective space L, h be a rational mapping of V onto a variety W and H be the graph of h. Let $\mathfrak{D}$ be a closed subset of V such that h is defined everywhere on $V - \mathfrak{D}$, and W_0 be the set-theoretic image of $V - \mathfrak{D}$ by h. Let k be a common field of definition for V and h over which $\mathfrak{D}$ is normally algebraic. Then W_0 is a k-open set on W if the following conditions are satisfied:*

(i) *Whenever w' is a point of W_0, $V \times w' \cap H$ contains a component of dimension $t = \dim V - \dim W$, containing a point $v' \times w'$ such that $v' \in V - \mathfrak{D}$;*

(ii) *Denoting by $\mathfrak{F} \times w'$ the maximal algebraic set of dimension t in $V \times w' \cap H$, there is a specialization $(w, h^{-1}(w)) \rightarrow (w', Y')$ref. k such that $v' \in |Y'| \subset \mathfrak{F}$.*

Proof. By Weil [20], Appendix, Prop. 10, W_0 contains a k-open set and the union W' of all such sets is also k-open. Let W^* be the derived normal variety of W with reference to $\bar{k}$ and f be the birational transformation of W to W^* defined by the normalization. Put $h^* = f \cdot h$, then it is a rational mapping of V onto W^* with a field of definition $\bar{k}$. Let x, x' be Chow-points of $h^{-1}(w)$, Y' and M be the locus of x over $\bar{k}$. Since $\bar{k}(w) \supset \bar{k}(x)$, there is a rational mapping g from W onto M such that $g(w) = x$. Put $g^* = g \cdot f^{-1}$. Our assumptions (i), (ii) imply that $w' \times x'$ is an isolated component of $G \cap w' \times M$, where G is the graph of g. Denote by G^* the graph of g^*. Since f^{-1} is defined everywhere on W^* and since any point on W has only a finite set of images by f (cf. Zariski [23]), it follows that there is a point w'^* on W^* with $f^{-1}(w'^*) = w'$ such that $G^* \cap w'^* \times M$ has an isolated component $w'^* \times x'$. Hence by the main theorem on birational transformations (cf. Zariski [23]), g^* is defined at w'^*.

Let X be a component of $W - W'$ containing w', assuming that w' is in W_0 but not in W'. There is a subvariety X^* defined over $\bar{k}$ on W^*, going through w'^* such that X is the image of X^* by f^{-1}. Then g^* is defined at a generic point w''^* of X^* over $\bar{k}$ (Weil [16], Chap. IV, Cor., Th. 15). $g^*(w''^*)$ is the Chow-point of a cycle Y'' in L such that $Y'' \rightarrow Y'$ ref. $\bar{k}$; $|Y''|$ contains a point v'' such that $(Y'', v'') \rightarrow (Y', v')$ ref. $\bar{k}$. Since $v' \notin \mathfrak{D}$, v'' is not contained in $\mathfrak{D}$. Let H^* be the graph of h^*. There is a $\bar{k}$-closed subset $\mathfrak{E}^*_1$ on X^* such that $\mathfrak{E}^*_1$ is the set of points on X^* where g^* is not defined; there is also a $\bar{k}$-closed set $\mathfrak{E}^*_2$ on X^* such that $\mathfrak{E}^*_2$ is the set of points on X^* which have the property that $|H^* \cap V \times w^*_2| \subset |\mathfrak{D} \times W^*|$ (cf. Weil [20], Appendix, Prop. 8; Weil [18], Lemma 7). Since $w''^* \notin \mathfrak{E}^*_1 \cup \mathfrak{E}^*_2 = \mathfrak{E}^*$, $\mathfrak{E}^*$ is a proper $\bar{k}$-closed subset of X^*. Let $\mathfrak{E}$ be the image of $\mathfrak{E}^*$ by f^{-1}, then it is a proper $\bar{k}$-closed subset of X. Let $\bar{w}$ be a point of $X - \mathfrak{E}$. There is a point $\bar{w}^*$ in $X^* - \mathfrak{E}^*$ such that $f^{-1}(\bar{w}^*) = \bar{w}$. Hence g^* is defined at $\bar{w}^*$ and the cycle $\bar{Y}$ in L, whose Chow-point is $g^*(\bar{w}^*)$, contains a point $\bar{v}$ in $V - \mathfrak{D}$. Since $|\bar{Y} \times \bar{w}^*| \subset |H^* \cap V \times \bar{w}^*|$, it follows that $|\bar{Y} \times \bar{w}| \subset |H \cap V \times \bar{w}|$. Hence h is defined at $\bar{v}$ and $h(\bar{v}) = \bar{w}$. This proves that $W' \subsetneqq W' + X - \mathfrak{E} \subset W_0$. Let α be any automorphism of $\bar{k}$ over k. Since $X - \mathfrak{E} \subset W_0$, it follows that $(X - \mathfrak{E})^\alpha \subset W_0$. Consequently there is a k-open set W'' on W such that $W' \subsetneqq W'' \subset W_0$, which contradicts to our choice of W' and our lemma is thereby proved.

7. Let U be a complete variety, non-singular in co-dimension 1, and let $\mathfrak{X}$ be a set which can put a structure of polarization on U. Let f_X be a non-degenerate projective embedding of U determined by a linearly effective divisor X in $\mathfrak{X}$, and denote by $c(f_X(U))$ the Chow-point of $f_X(U)$, except when U is an abelian variety. When U is an abelian variety with the neutral element O, denoting by U' the underlying variety of the abelian variety U, we understand by $c(f_X(U))$ a pair $(x, f_X(O))$ of points, where x is the Chow-point of $f_X(U')$. Let $\mathfrak{S}$ be a subset of $\mathfrak{X}$, then we shall say that $\mathfrak{P}(U, \mathfrak{S})$ has a *structure of an algebraic variety* when the set of points $c(f_X(U))$, with $f_X(U)$ in $\mathfrak{P}(U, \mathfrak{S})$, forms an open algebraic variety. When that is so, we shall say that $\mathfrak{P}(U, \mathfrak{S})$ is defined over a field k if the open algebraic variety is defined over k.

THEOREM 3. *Let U be a non-singular variety in a projective space and $\mathfrak{A}$ be a complete family of algebraically effective positive U-divisors. Then*

$\mathfrak{P}(U, \mathfrak{A})$ has a structure of an algebraic variety. The same is true when U is an abelian variety. In both cases, $\mathfrak{P}(U, \mathfrak{A})$ is defined over a common field of definition for U and $\mathfrak{A}$; moreover $\mathfrak{P}(U, \mathfrak{A})$ has the smallest field of definition if $\mathfrak{A}$ is total.

Proof. Let us assume first that U is an abelian variety and let U' be the underlying variety of U. We shall show that $\mathfrak{P}(U, \mathfrak{A})$ has a structure of an algebraic variety when $\mathfrak{P}(U', \mathfrak{A})$ has a structure of an algebraic variety. Let W be the set of points $c(f(U'))$, where f is a non-degenerate projective embedding of U' determined by a divisor in $\mathfrak{A}$. Assume that W is an open algebraic variety and let k be a field of definition for W. When w is a generic point of it over k, it is the Chow-point of a variety of the form $f(U')$ in $\mathfrak{P}(U', \mathfrak{A})$, which is defined over $k(w)$. By Weil [16], Chap. VII, Th. 12, there is the uniquely determined subvariety Z on the product $W \times L$ of W with the ambient space of $f(U')$ such that $Z(w) = f(U')$. Let w' be a point on W and let $f'(U')$ be the corresponding variety in $\mathfrak{P}(U', \mathfrak{A})$. Let u' be a point on $f'(U')$, then there is a non-degenerate projective embedding g' of U' determined by a divisor in $\mathfrak{A}$ such that $g'(U') = f'(U')$ and that when O is the neutral element of U, $g'(O) = u'$. Hence $g'(U)$ is the abelian variety with the neutral element u' whose underlying variety is $g'(U')$, which proves that $c(g'(U)) = (w', u')$. Conversely, let f'' be a non-degenerate projective embedding of U determined by a divisor in $\mathfrak{A}$. $f''(U)$ is an abelian variety with the neutral element $f''(O)$ and let w'' be the Chow-point of the underlying variety of $f''(U)$. Then by our assumption, w'' is a point of W and hence $(w'', f''(O))$ is a point of Z. Thus $|Z|$ coincides with the set of points $c(f''(U))$. Our assertion is thereby proved.

Let us return to our general case when U is an ordinary non-singular variety in a projective space. Let k be a common field of definition for U and $\mathfrak{A}$, then the set of Chow-points of non-degenerate projective embeddings determined by divisors in $\mathfrak{A}$ forms an open algebraic variety $V - \mathfrak{D}$ in a projective space defined over k (cf. Lemma 4), where V is a projective variety, and $\mathfrak{D}$ is a k-closed set on V. Let v be a point on $V - \mathfrak{D}$ and f be the corresponding projective embedding of U. When w is the Chow-point of $f(U)$, we shall write U_w, f_w, t_w for $f(U), f, v$, for the sake of simplicity. Let us now assume that v is a generic point of V over k. Since $k(v) \supset k(w)$, w has a locus W over k, which is the closure of the point set $\{c(U^*)\}$ with U^* in $\mathfrak{P}(U, \mathfrak{A})$, and there is a rational mapping h of V onto W such that $h(v) = w$. Let U^* be a variety in $\mathfrak{P}(U, \mathfrak{A})$, a be the Chow-point of U^* and t_a be one of the points on $V - \mathfrak{D}$ such that the corresponding non-degenerate embedding f_a transforms U to $U^* = U_a$. Let t_w, t_s be two independent generic points of V over $k(t_a, a)$ and let k' be the algebraic closure of $k(t_a, t_s)$. Let f_w, f_s be corresponding non-degenerate projective embeddings of U to t_w, t_s; put $f_{w,s} = f_w \cdot f_s^{-1}$, $f_{s,w} = f_s \cdot f_w^{-1}$ and let $t_{w,s}, t_{s,w}$ be Chow-points of $f_{w,s}, f_{s,w}$ respectively. Let t'_w be a generic point of $h^{-1}(w)$ over $k'(w)$, f'_w be the corresponding embedding of U and let t'_s be the Chow-points of $f_{s,w} \cdot f'_w$. By Lemma 3, t'_s is also on $V - \mathfrak{D}$ and let Z be the locus of $(t_w, w, t_{s,w}, t'_w, t'_s)$ over k'. Z is then a subvariety of $V \times W \times L \times V \times V$ where L is the ambient space of $t_{s,w}$.

Let $\mathfrak{F}$ be the projection of $(t_a, a) \times L \times V \times V \cap Z$ on the fourth factor of the product. We claim that $\mathfrak{F}$ has the following three properties: (i) Every component of $\mathfrak{F}$ has the same dimension as $h^{-1}(w)$; (ii) Every component of $\mathfrak{F}$ is not contained in $\mathfrak{D}$; (iii) $\mathfrak{F}$ is the closure on V of the set of points t'_a on V corresponding to non-degenerate embeddings of U, transforming U to U_a. Let (t_a, a, u, t, x) be a point in $(t_a, a) \times L \times V \times V \cap Z$. By Lemma 3 and by the compatibility of specializations with the operations of intersection-product and algebraic projection, we see that u is the Chow-point of $f_s \cdot f_a^{-1} = f_{s,a}$ since $t_{s,w}$ is the Chow-point of $f_s \cdot f_w^{-1}$. Let $T_{s,a}$ be the graph of $f_{s,a}$ and T be the cycle whose Chow-point is t. Since t'_s is the Chow-point of $f_{s,w} \cdot f'_w$, it follows that x is the Chow-point of $T_{s,a} \circ T$. Since t'_s is contained in $|h^{-1}(s)|$, it follows that x is also contained in it. By Lemma 3, the correspondence $T \rightarrow T_{s,a} \cdot T$ gives a one-to-one correspondence between points of $\mathfrak{F}$ and points of a subset of $|h^{-1}(s)|$. This shows that the dimension of each component of $\mathfrak{F}$ is at most that of $h^{-1}(s)$. Since f_s, f_a are defined over k', $f_{s,a} = f_s \cdot f_a^{-1}$ is defined over k' and consequently the Chow-point $u = t_{s,a}$ of $f_{s,a}$ is rational over k'. Therefore we get $\dim_{k'}(u, t, x) = \dim_{k'}(t)$ by Lemma 3. Since $Z \cap (t_a, a) \times L \times V \times V$ has not any component of lower dimension than that of $Z \cap (t_w, w) \times L \times V \times V$ by Weil [16], Chap. IV, Prop. 26, which is obviously the same as $\dim h^{-1}(w) = \dim h^{-1}(s)$, our statement (i) is proved. By Lemma 3, if $T_{s,a} \circ T$ is an isomorphism, so is T. Therefore, every component of $\mathfrak{F}$ contains the Chow-point of an isomorphism of U onto U_a and since $\mathfrak{A}$ is complete, it must be non-degenerate. This proves (ii). Let t'_a be a point on $V - \mathfrak{D}$ such that the corresponding embedding f'_a transforms U to U_a. In order to prove (iii), it is sufficient to prove that the projection of $Z \cap (t_a, a) \times L \times V \times V$ on the last factor of the product is $|h^{-1}(s)|$, since the Chow-point of $f_{s,a} \cdot f'_a$ is on $|h^{-1}(s)|$ and since the correspondence $f_s \rightarrow f_{s,a}^{-1} \cdot f_s$ determines a one-to-one correspondence between point of $|h^{-1}(s)|$ and points of a subset of $\mathfrak{F}$ as before for the fixed $f_{s,a}$. By Lemma 3, the projection of $Z \cap (t_w, w) \times L \times V \times V$ on the fifth factor is $|h^{-1}(s)|$, hence the same is true for $Z\cap(t_a, a)\times L\times V\times V$. (iii) is thereby proved.

Let V' be the locus of (t_w, w) over k', then since $h(t_w)=w$, V' is also the locus of (t_w, w) over k. Let $\mathfrak{D}'$ be the set of points (t', c) on V' such that $t'\in\mathfrak{D}$. Then $\mathfrak{D}'$ is also a closed subset of V' over k. Let h' be the rational mapping of V' onto W defined by $h'(t_w, w)=w$. h' is defined everywhere on $V'-\mathfrak{D}'$ and the set-theoretic image W_0 of $V'-\mathfrak{D}'$ by h' is the point-set we are interested in. We are going to show that to V', $\mathfrak{D}'$ and h', our Lemma 5 can be applied. Let $(t_w, w, h'^{-1}(w))\rightarrow(t_a, a, Y)$ ref. k', where we assume now that a is a point on W_0. We have $h'^{-1}(w)=h^{-1}(w)\times w$, and since $\mathrm{pr}_4(Z\cdot((t_w, w)\times L\times V\times V))=h^{-1}(w)$, $|Y|$ is contained in $\mathfrak{F}\times a$. Since $\dim Y=\dim h^{-1}(w)=\dim\mathfrak{F}$ by (i), every component of Y contains a point of $V'-\mathfrak{D}'$ by (ii). Moreover, we see from this that every component of $Y\times a$ is a component of $H'\cap V'\times a$, where H' is the graph of h'. Therefore we can apply our Lemma 5 and thus W_0 is an open algebraic variety over k in a projective space. Thus the first half of our theorem is proved.

Let k_0 be the smallest field of definition for W. We shall show that W_0 is defined over k_0, which will settle the last half of our theorem. Let w be a generic point of W over k_0 and f_w be a non-degenerate embedding of U into the projective space, transforming U to U_w. It is easy to see that $\mathfrak{P}(U,\mathfrak{A})=\mathfrak{P}(U_w, f_w(\mathfrak{A}))$. $f_w(\mathfrak{A})$ contains a rational divisor over $k_0(w)$, a hyperplane section of U_w, and since $f_w(\mathfrak{A})$ is complete and total, it is easy to see that $f_w(\mathfrak{A})$ is defined over a purely inseparable extension of $k_0(w)$. Let us take for $U, \mathfrak{A}$ the variety U_w and the family $f_w(\mathfrak{A})$. Since W and W_0 are invariants of $\mathfrak{P}(U,\mathfrak{A})=\mathfrak{P}(U_w, f_w(\mathfrak{A}))$, it follows that $W-W_0$ is normally algebraic over $k_0(w)$. Let w' be a generic point of W over $k_0(w)$. Then in the same way, we can show that $W-W_0$ is normally algebraic over $k_0(w')$, hence $W-W_0$ is normally algebraic over k_0. Our theorem is thereby proved completely.

Section 3.

8.

PROPOSITION 4. *Let U be a variety in a projective space, non-singular in co-dimension* 1, *and $\mathfrak{X}$ be a set of divisors on U which defines a polarization on it. There is a divisor class $\mathfrak{N}^*$ with respect to numerical equivalence with the following property: A positive U-divisor X belongs to $\mathfrak{X}$ if and only if X belongs to $m\mathfrak{N}^*$ for a certain positive integer m.*

Proof. By Néron's result, $G(U)/G_a(U)$ is finitely generated (Néron [10]). On the other hand, $G_n(U)/G_a(U)$ is a subgroup of $G(U)/G_a(U)$, consisting of elements of finite orders. Therefore, there is a finite set $(D_1, \cdot\cdot, D_s)$ of divisors on U, which are independent modulo $G_n(U)$, such that any U-divisor X can be written as $X \equiv \sum c_i D_i \bmod G_n(U)$. Let Y be a divisor in $\mathfrak{X}$, then expressing Y in the form $Y \equiv \sum a_i D_i \bmod G_n(U)$, let b be the greatest common divisor of $a_1, \cdot\cdot\cdot, a_s$. Putting $a_i = b \cdot a'_i$, let $\mathfrak{N}^*$ be the coset of $G(U) \bmod G_n(U)$ determined by $Z = \sum a'_i D_i$. Let m be a positive integer and X be a positive divisor in $m\mathfrak{N}^*$. Clearly X is contained in $\mathfrak{X}$ by the definition of $\mathfrak{X}$. Conversely, let X be any divisor in $\mathfrak{X}$. There are two positive integers m and t such that $mY \equiv tX \bmod G_n(U)$ and that m and t are relatively prime to each other. Then $bmZ \equiv tX \bmod G_n(U)$. Expressing X as $X \equiv \sum c_i D_i \bmod G_n(U)$, we see that $\sum (bma'_i - tc_i) D_i \equiv 0 \bmod G_n(U)$, which implies that $bma'_i \equiv 0 \bmod t$. Therefore $mb \equiv 0 \bmod t$ since $(a'_1, \cdot\cdot\cdot, a'_s)$ is a set of relatively prime integers. Our proposition is thereby proved.

THEOREM 4. *Let V be a complete non-singular variety, polarized by a set $\mathfrak{X}$. $\mathfrak{X}$ can be written as $\bigcup \mathfrak{A}(X)$ with X in $\mathfrak{X}$. Let $\mathfrak{X}^*$ be the set of divisors X in $\mathfrak{X}$ such that $\mathfrak{A}(X)$ is complete, total and consists of algebraically effective divisors. Then $\mathfrak{X}^*$ can also be written as $\bigcup \mathfrak{A}(X)$ with X in $\mathfrak{X}^*$. Every $\mathfrak{A}(X)$ in the expression for $\mathfrak{X}$, except for a finite set of them, is also a component of the same expression for $\mathfrak{X}^*$. $\mathfrak{P}(V, \mathfrak{X})$* (resp. $\mathfrak{P}(V, \mathfrak{X}^*)$) *is the union of $\mathfrak{P}(V, \mathfrak{A}(X))$, where $\mathfrak{A}(X)$ is a component of $\mathfrak{X}$* (resp. $\mathfrak{X}^*$). *Moreover, when V is an abelian variety, $\mathfrak{P}(V, \mathfrak{X})$ and $\mathfrak{P}(V, \mathfrak{X}^*)$ coincide.*

Proof. The first two statements about expressions for $\mathfrak{X}$ and $\mathfrak{X}^*$ are immediate consequences of definitions.

Since $\mathfrak{X}$ contains a linearly effective divisor by our definition, we may assume that $\mathfrak{X}$ is determined by a hyperplane section of a variety V in a projective space. Let C be a hyperplane section of V. There is the divisor class $\mathfrak{N}^*$ with respect to numerical equivalence having the property described in Proposition 4. Let Z be a divisor in $\mathfrak{N}^*$, then there is a positive integer s such that $C \equiv sZ \bmod G_n(V)$. By Theorem 1, (ii), there is a positive integer m_0 such that whenever $m > m_0$, $\mathfrak{N}(iZ + mC)$ is covered by a finite set of complete total families and that $iZ + mC$ is numerically effective for $0 \leqq i \leqq s-1$. Put $t = m_0 s$, then $m_0 C \equiv tZ \bmod G_n(V)$. We shall show that $\mathfrak{N}(t'Z)$ is not empty, consists of numerically effective divisors and is covered by a finite set of complete total families whenever $t' > t$. In fact,

$t'Z \equiv atZ + bsZ + cZ \bmod G_n(V)$, where a is a positive integer, b and c are non-negative integers and c is less than s. Therefore we have $t'Z \equiv (am_0 + b)C + cZ \bmod G_n(V)$ which should be numerically effective and $\mathfrak{N}(t'Z)$ is covered by a finite set of complete total families by our choice of m_0. Therefore our third assertion is proved.

Our fourth assertion is trivial. In order to prove the last assertion, it is sufficient to show that when X is a linearly effective divisor on an abelian variety, $\mathfrak{A}(X)$ is complete, total and X is algebraically effective, which are consequences of Proposition 2.

THEOREM 5. *Let V be a complete non-singular variety, polarized by a set $\mathfrak{X}$. Then every polarized variety in $\mathfrak{P}(V, \mathfrak{X})$, polarized by the natural polarization, is isomorphic to each other. When V is an abelian variety, underlying varieties of polarized abelian varieties in $\mathfrak{P}(V, \mathfrak{A})$ are projectively equivalent to each other, where $\mathfrak{A}$ is a divisor class of $V \bmod G_a(V)$ contained in $\mathfrak{X}^*$.*

Proof. The first statement is obvious. Assume that V is an abelian variety and A, A' be two polarized abelian varieties in $\mathfrak{P}(V, \mathfrak{A})$, polarized by natural polarizations, with neutral elements O, O'. Let us identify A, A' with their underlying varieties. There is an isomorphism f between two polarized abelian varieties A, A', which is determined by a divisor on A, algebraically equivalent to a hyperplane section C of A. Let Y be such a positive divisor on A, then $f(Y)$ is a hyperplane section of A', and $f(C) \equiv f(Y) \bmod G_a(A')$. Since $f(C)$ is non-degenerate by Proposition 2, there is a point a' on A' such that $f(C)_{a'} \sim f(Y)$. Hence, denoting by T the translation on A' defined by a', we have $T \cdot f(C) \sim f(Y)$. Moreover, $T \cdot f$ is an isomorphism between two polarized varieties A, A' and transforms hyperplane sections to hyperplane sections. Since linear systems of hyperplane sections on A and A' are complete, $T \cdot f$ must be a projective transformation of A onto A'. Our theorem is thereby proved.

9. Let U be a complete non-singular variety, polarized by a set $\mathfrak{X}$. We shall denote by $\mathfrak{G}(U, \mathfrak{X})$ the group of automorphisms of the polarized variety U. Let W be also a complete non-singular polarized variety, polarized by a set $\mathfrak{Y}$ and assume that f is an isomorphism between polarized varieties U and W. Then it is easy to see that the correspondence $g \to f \cdot g \cdot f^{-1}$, $g \in \mathfrak{G}(U, \mathfrak{X})$ gives an isomorphism of $\mathfrak{G}(U, \mathfrak{X})$ and $\mathfrak{G}(W, \mathfrak{Y})$.

PROPOSITION 5. *Let U^n be a projective variety, non-singular in codimension 1, and G^r be a connected algebraic group variety. Let Z^{n+r} be a* *subvariety of* $G \times U \times U$ *and assume that the projection of* Z *on* $G \times U$ *is* $G \times U$ *and is everywhere regular, where* U *is any one of the second and the third factors of* $G \times U \times U$. *Then for any point* g *on* G, $(g \times U \times U) \cdot Z$ *is defined and* $Z(g)$ *is the graph of an automorphism of* U. *Further, denote by* Y^g *the transform of a* U*-cycle* Y *by* $Z(g)$ *and assume that* $u^e = u$ *for any point* u *on* U, *where* e *is the neutral element of* G. *Then we have the following:* (i) *When* X *is a* U*-divisor,* $X^g \equiv X \bmod G_a(U)$; (ii) *When* X *is a* U*-divisor such that* $X \equiv 0 \bmod G_a(U)$, $X^g \sim X$.

Proof. Let $g \times T$ be a component of $g \times U \times U \cap Z$, which is simple on $G \times U \times U$. Let (u, v) be a point on T; by our definition of Z, v is uniquely determined by g and u, hence $\dim T \leqq \dim U$, which proves our assertion. Then it is clear that $Z(g)$ is the graph of an automorphism of U. Next, we claim that $Z \cdot (G \times X \times U) = Z'$ is defined on $G \times U \times U$. Let (g, x, u) be any point in $Z \cap G \times X \times U$; then $u = x^g$ and this shows that the dimension of any component of our intersection must be at most $r + n - 1$, which proves our assertion. Therefore by Weil [16], Chap. VII, Cor., Th. 10, we see that

$$\begin{aligned}((g \times U \times U) \cdot Z) \cdot (G \times X \times U)& \\ = (g \times U \times U) \cdot (Z \cdot (G \times X \times U)) &= g \times Z(g) \cdot (X \times U).\end{aligned}$$

$Z \cdot (G \times X \times U)$ can be regarded as a cycle on $G \times L \times U$, where L is the ambient space of U, then by Weil [16], Chap. VII, Th. 18, we see that

$$\begin{aligned}\{(g \times L \times U) \cdot (Z \cdot (G \times X \times U))\}_{G \times L \times U}& \\ = (g \times U \times U) \cdot (Z \cdot (G \times X \times U)).&\end{aligned}$$

That being so, by Weil [16], Chap. VII, Th. 16, we have

$$\mathrm{pr}_{13}((g \times U \times U) \cdot (Z \cdot (G \times X \times U))) = (g \times U) \cdot \mathrm{pr}_{13}(Z \cdot (G \times X \times U)).$$

Therefore

$$(g \times U) \cdot \mathrm{pr}_{13}(Z \cdot (G \times X \times U)) = g \times \mathrm{pr}_3(Z(g) \cdot (X \times U)) = g \times X^g.$$

By taking g to be e, we get $(e \times U) \cdot \mathrm{pr}_{13}(Z \cdot (G \times X \times U)) = e \times X^e = e \times X$, which proves that $X^g \equiv X \bmod G_a(U)$. (i) is thereby proved.

Let $\mathfrak{F}$ be a total maximal family of positive U-divisors, V be the Chow variety of $\mathfrak{F}$ (the set of Chow-points of divisors in $\mathfrak{F}$) and denote by Y_v the divisor whose Chow-point is $v \in V$. Let $P(U)$ be the Picard variety of U and γ be the canonical homomorphism of $G_a(U)$ onto $P(U)$. Let k be an algebraically closed common field of definition for $U, G, Z, V, P(U)$ and γ

over which X is rational. By (i), $Z(g)^{-1}(Y_v) \equiv Y_v \bmod G_a(U)$ and hence the mapping $(g,v) \to \gamma(Z(g)^{-1}(Y_v) - Y_v)$ defines a rational mapping of $G \times V$ into $P(U)$ with a field of definition k (Y_v is rational over $k(v)$; cf. W. L. Chow, "On the defining field of a divisor in an algebraic variety," *Proc. Amer. Math. Soc.*, vol. 6, 1950), which we shall denote by F. Assume that g and v are independent generic points of G and V over k, then F can be written as $F(g,v) = F_1(g) + F_2(v)$, where F_1 is a rational mapping of G into $P(U)$ and F_2 is a rational mapping of V into $P(U)$ (cf. Weil [17], Cor., Th. 7), both defined over k. Since $F(g,v)$ has the uniquely determined specialization $\gamma(Z(e)^{-1}(Y_v) - Y_v)$ over $(g,v) \to (e,v)$ ref. $k(v)$, and since (e,v) is a simple point on $G \times V$, F is defined at (e,v) (cf. Weil [16], Chap. VI, Th. 13). Therefore, we have

$$F(e,v) = \gamma(Z(e)^{-1}(Y_v) - Y_v) = Z(Y_v - Y_v) = O,$$

which proves that $F_2(v) = -F_1(e)$ is a constant, rational over k. By the compatibility of specializations with the operations of intersection-product and algebraic projection, we see that F is single-valued everywhere on $G \times V$ and has the value $\gamma(Z(g)^{-1}(Y_w) - Y_w)$ at (g,w). Hence we have

$$\gamma(Z(g)^{-1}(Y_v) - Y_v) = \gamma(Z(g)^{-1}(Y_w) - Y_w),$$

whenever w is a generic point of V over $k(g,v)$. Consequently

$$\gamma(Z(g)^{-1}(Y_t) - Y_t) = \gamma(Z(g)^{-1}(Y_s) - Y_s)$$

for any two points t, s on V. Let now X be a U-divisor such that $X \equiv 0 \bmod G_a(U)$, then since $\mathfrak{F}$ is total, there are two points t and s on V such that $Y_t - Y_s \sim X$. By what we have proved, we have $(Y_t - Y_s)^g \sim Y_t - Y_s$ and since $X^g \sim (Y_t - Y_s)^g$, it follows that $X^g \sim X$. Our proposition is thereby proved.

10.

LEMMA 6. *Let U be a normal variety in a projective space, C be a hyperplane section of U and assume that $\mathfrak{A}(C)$ is a complete algebraic family of algebraically effective divisors and that the linear system of hyperplane sections on U is complete. Let Σ be the set of automorphisms f of U such that $f(C) \in \mathfrak{A}(C)$, and W be the set of Chow-points of f. Then $W = \bigcup_0^m W_i$, where the W_i are open algebraic varieties in a projective space. When U and $\mathfrak{A}(C)$ are defined over a field k, then W is normally algebraic over k.*

Proof. Let V be the set of Chow-points of graphs of non-degenerate projective embeddings determined by divisors in $\mathfrak{A}(C)$. Then by our Lemma 4, V is an open algebraic variety in a projective space L. Let f be an automorphism of U such that $f(C) \in \mathfrak{A}(C)$. Then since f is everywhere biregular, $f^{-1}(C) \in \mathfrak{A}(C)$; since $\mathfrak{A}(C)$ is complete, every divisor in it determines a complete linear system of the same dimension as C. Therefore, f is a non-degenerate projective embedding determined by $f^{-1}(C)$ and the Chow-point of it is on V. Let k be a common field of definition for U and $\mathfrak{A}(C)$, then V is an open algebraic variety in L over k by Lemma 4. Let v be a generic point of V over k and T_v be the variety with the Chow-point v. T_v is the graph of a non-degenerate projective embedding of U, determined by a generic divisor of $\mathfrak{A}(C)$ over k and is defined over the field $k(v)$. Therefore, there is a subvariety T of $V \times U \times \bar{L}$, where $\bar{L}$ is the ambient space of U, such that $T(v) = T_v$ and that k is a field of definition for T (cf. Weil [16], Chap. VII, Th. 12). Let $\mathfrak{F} = T \cap V \times U \times \bar{U}$. $\mathfrak{F}$ is a closed algebraic set, normally algebraic over k on $V \times U \times \bar{L}$. Let w be a point on V and T_w be the corresponding subvariety of $U \times \bar{L}$, then since T_w is the uniquely determined specialization of T_v over $v \rightarrow w$ ref. k, it follows that $T \cap w \times U \times \bar{L}$ reduces to a component $w \times T_w$. When T_w is the graph of an automorphism of U, $w \times T_w$ is a subvariety of $V \times U \times U$ and hence $\mathfrak{F} \cap w \times U \times \bar{L}$ contains $w \times T_w$. Conversely, assume that $\mathfrak{F} \cap w \times U \times \bar{L}$ contains a component $w \times R$ of at least the same dimension as U. Then since $w \times R$ is a subvariety of T, we have $w \times R \subset w \times T_w$. Since $\dim R \geqq \dim T_w$, it follows that $R = T_w$ and the projection of T_w on $\bar{L}$ is U. Therefore T_w must be the graph of an automorphism of U. Thus we have shown that the set of points w on V, such that T_w is the graph of an automorphism of U, coincides with the set of points on V such that $w \times U \times \bar{L} \cap \mathfrak{F}$ contains a component of dimension at least equal to that of U. Such a set forms a closed algebraic set on V, normally algebraic over k by Weil [18], Lemma 7. Our lemma is thereby proved.

LEMMA 7. *Maintaining the same notations and assumptions as in the preceding lemma, denote also by* T_{w_i} *the subvariety of* $U \times U$ *with the Chow-point* w_i *on* W_i. *Let* W_0 *be a component of* W *containing the Chow-point of the diagonal of* $U \times U$. *Then we have the following results:*

(i) $\dim W_0 = \dim W_1 = \cdots = \dim W_m$;

(ii) $W_i \cap W_j = \emptyset$ *whenever* $i \neq j$;

(iii) *Let* w_i *and* w_j *be points of* W_i *and* W_j *respectively, then* $T_{w_j} \circ T_{w_i}$ *is the graph of an automorphism of* U *belonging to* Σ;

(iv) *Let* k_{ij} *be a common field of definition for* W_i *and* W_j *containing* k, w_i *and* w_j *be independent generic points of* W_i *and* W_j *over* k_{ij} *and let* W_s *be a component of* W *containing the Chow-point* w_s *of* $T_{w_j} \circ T_{w_i}$, *then* s *is a function* $\alpha(i,j)$ *of* (i,j) *only and* (w_i, w_j, w_s) *has a locus* Z_{ijs} *over* k_{ij};

(v) *Projections of* Z_{ijs} *on* $W_i \times W_j$, $W_i \times W_s$ *and on* $W_j \times W_s$ *are regular and surjective*;

(vi) *Let* v_i, v_j, v_s *be arbitrary points on* W_i, W_j, W_s *respectively, then* $(v_i, v_j) \times W_s \cap Z_{ijs}$, $v_i \times W_j \times v_s \cap Z_{ijs}$ *and* $W_i \times (v_j, v_s) \cap Z_{ijs}$ *have single zero-dimensional components*;

(vii) $\alpha(0,j) = \alpha(j,0) = 0$.

Proof. By Lemma 3, $T_{w_j} \circ T_{w_i}$ is defined and is again the graph of an automorphism of U, since T_{w_i}, T_{w_j} are such. Since $T_{w_i}(C) \equiv T_{w_j}(C) \equiv C \bmod G_a(U)$, we see that $T_{w_j} \circ T_{w_i}(C) \equiv C \bmod G_a(U)$. (iii) is thus proved. Let now w_i and w_j be independent generic points of W_i and W_j over k_{ij}, then the Chow-point w_s of $T_{w_j} \circ T_{w_i}$ is rational over $k_{ij}(w_i, w_j)$ by Lemma 3. Hence (w_i, w_j, w_s) has a locus Z_{ijs} over k_{ij} on $W_i \times W_j \times W_s$. Let (v_i, v_j) be an arbitrary point on $W_i \times W_j$, then $T_{v_j} \circ T_{v_i}$ is the uniquely determined specialization of $T_{w_j} \circ T_{w_i}$ over $(w_i, w_j) \rightarrow (v_i, v_j)$ ref. k_{ij} by Lemma 3 and by Lemma 6. This shows that $\alpha(i,j)$ actually depends only on i and j as soon as we prove (ii). Moreover, we have shown that $Z_{ijs} \cap (v_i, v_j) \times W_s$ reduces to a point and the projection of Z_{ijs} on $W_i \times W_j$ is regular and surjective. Next let us show, among other things, that W_0 is the unique component of W containing the Chow-point of Δ. Let W_i be a component of W and put $\alpha(0,i) = j$. Since the projection of Z_{0ij} on W_j contains W_i because $T_{v_i} \circ \Delta = T_{v_i}$, it follows that $W_i = W_j$ proving that $\alpha(0,i) = i$. In the same way, $\alpha(0,i) = i$. Suppose now that W_i contains also the Chow-point of Δ. Then W_i contains W_0 since $\alpha(0,i) = i$ and consequently $W_i = W_0$.

The formula $\alpha(0,i) = i$ shows that $\dim W_0 \leqq \dim W_i$ by virtue of Lemma 3. Conversely, let w_i be a generic point of W_i over k_{0i}. Then the set of Chow-points of $T_{w_i}^{-1} \circ T_{v_i}$, where v_i is a point on W_i, is contained in $|W|$ and forms an open algebraic variety in the ambient space of W. Since it contains the Chow-point of Δ, it must be contained in W_0 by what we have seen, proving that $\dim W_0 \geqq \dim W_i$ (cf. Lemma 3). Thus (i) is proved.

Let a be a common point of W_i and W_j and w_i, w_j be independent generic points of W_i, W_j over $k_{ij}(a)$ respectively. Since Δ is a specialization of both $T_{w_i} \circ T_a^{-1}$, $T_{w_j} \circ T_a^{-1}$ over $k_{ij}(a)$, it follows that Chow-points of them are on W_0. Since $\dim W_0 = \dim W_i = \dim W_j$, it follows that $T_{w_i} \circ T_a^{-1}$, $T_{w_j} \circ T_a^{-1}$

are generic specializations of each other over $k_{ij}(a)$, which shows that T_{w_i} and T_{w_j} are generic specializations of each other over k_{ij}. Therefore $W_i = W_j$ and (ii) is thus proved. Now (v) and (vi) are easy consequences of what we have proved.

11.

THEOREM 6. *Let U be a complete non-singular polarized variety, polarized by a set $\mathfrak{X}$. Then there is an algebraic group $G = \bigcup_0^m G_i$, where G_0 is the connected component of G containing the neutral element e and the G_i are cosets of G_0, and subvarieties Z_i of $G_i \times U \times U$ with the following properties:*

(i) *Projections of Z_i on the product of G_i and the second factor and also on that of G_i and the third factor are everywhere regular;*

(ii) *$(g_i \times U \times U) \cdot Z_i = g_i \times Z_i(g_i)$ is defined for all g_i on G_i and in particular $Z_0(e) = \Delta$;*

(iii) *$Z_i(g_i) = Z_j(g'_j)$ implies $i = j$ and $g_i = g'_j$;*

(iv) *The group of automorphisms $\mathfrak{G}(U, \mathfrak{X})$ of U is the set of $Z_i(g_i)$ for all g_i on G_i and for all i* (we identify rational mappings and graphs);

(v) *When $g_j \cdot g_i = g_s \in G_s$, then $Z_s(g_s) = Z_j(g_j) \circ Z_i(g_i)$;*

(vi) *When our polarized variety U is defined over a field k_0 and when $\mathfrak{X}$ contains a rational divisor X_0 over k_0 which is linearly effective, then G is normally algebraic over k_0 and $\Sigma_i Z_i$ is rational over a finite purely inseparable extension of k_0.*

Proof. Let C be a linearly effective divisor in $\mathfrak{X}$ and k be a field of definition of U over which C is rational. By Weil [16], Chap. VIII, Th. 10, there is a non-degenerate projective embedding of U determined by C, defined over k. By our Th. 1, when r is sufficiently large, $\mathfrak{A}(rC)$ is a complete total algebraic family of algebraically effective divisors, and since it contains a rational divisor rC over k, $\mathfrak{A}(rC)$ is defined over k (cf. Matsusaka, [6], Prop. 1). Let f be any automorphism of U belonging to the set $\mathfrak{G}(U, \mathfrak{X})$, then $f(C) \equiv C \bmod G_n(U)$; since $G_n(U)/G_a(U)$ is a finite group (cf. Th. 1), $f(sC) \equiv sC \bmod G_a(U)$ whenever s is a positive integral multiple of the order of $G_n(U)/G_a(U)$. Therefore, we may assume, from the beginning, that U is a non-singular projective variety defined over k, $\mathfrak{X}$ contains a hyperplane section C of U, $\mathfrak{A}(C)$ is a complete total family of algebraically effective divisors and that every automorphism f in $\mathfrak{G}(U, \mathfrak{X})$ transforms C to a divisor in $\mathfrak{A}(C)$.

When that is so, f is a non-degenerate projective embedding of U determined by $f^{-1}(C)$ and our Lemmas 6, 7 can be applied. Hence the set W of Chow-points of $f \in \mathfrak{G}(U, \mathfrak{X})$ can be written as $\bigcup_0^m W_i$, where the W_i are open algebraic varieties in a projective space, and has properties described in Lemmas 6, 7. Let k' be the smallest perfect field containing k, then the W_i are defined over separable algebraic extensions k'_i of k'. Let G'_i be a derived normal variety of W_i with reference to k'_i and let G_i be the graph of the inverse of our normalization $W_i \rightarrow G'_i$. It is easy to see that the G_i can be so chosen that they are in the same space and that when γ is an automorphism of our universal domain over k, $W_i^\gamma = W_j$ implies $G_i^\gamma = G_j$. Then $\bigcup_0^m G_i$ forms an algebraic set normally algebraic over k. Since the k'_{ii}/k' are separable algebraic extensions, $\bigcup_0^m k'_i/k'$ is also a separable algebraic extension. Since the G_i are normal with reference to the k'_i, it follows that the G_i are still normal with reference to $K = \bigcup_0^m k'_i$ and the $G_i \times G_j$ are also normal with reference to K (cf. Weil [20], Appendix, Prop. 14). Therefore, if we assume (i), (ii), (iii), (iv), $\bigcup_0^m G_i$ is an algebraic group satisfying (v) by our Lemma 7, such that G_0 is the connected component of it containing the neutral element.

Let w_i be a generic point of W_i over k'_i and g_i be the corresponding point on G_i. Let T_{w_i} be the variety whose Chow-point is w_i, then it is the graph of an automorphism in $\mathfrak{G}(U, \mathfrak{X})$. Then T_{w_i} is defined over the field $k'_i(w_i) = k'_i(g_i)$ and hence there is a subvariety Z_i of $G_i \times U \times U$ defined over k'_i such that $Z_i(g_i) = T_{w_i}$ (cf. Weil [16], Chap. VII, Th. 12). Z_i is then the locus of $(g_i, u, T_{w_i}(u))$ over k'_i, where u is a generic point of U over $k'_i(g_i)$. (ii) is then an immediate consequence of the facts that the birational transformation $g_i \rightarrow w_i$ of G_i to W_i is everywhere defined on G_i and that specializations are compatible with the operation of intersection-product. Since the birational transformation $w_i \rightarrow g_i$ of W_i to G_i is such that any point on W_i has only a finite set of image points in G_i, (i) follows easily because $G_i \times U \times U$ is non-singular (cf. Weil [16], Chap. VI, Th. 13). In particular, when g'_i is a point on G_i and w'_i is the corresponding point on W_i, we have $Z_i(g'_i) = T_{w'_i}$, and conversely, if w'_i is a point on W_i and g'_i is one of the corresponding points on G_i, we have $Z_i(g'_i) = T_{w'_i}$. Therefore, the set of $Z_i(g'_i)$ with g'_i on G_i coincides with the set of varieties whose Chow-points are on W_i. Since any f in $\mathfrak{G}(U, \mathfrak{X})$ is a non-degenerate projective embedding of U determined by a divisor $f^{-1}(C)$, and conversely, any automorphism f' of U, such that $f'^{-1}(C)$ is in $\mathfrak{A}(C)$, is in $\mathfrak{G}(U, \mathfrak{X})$, it follows that $\mathfrak{G}(U,\mathfrak{X})$ coincides with the set of $Z_i(g'_i)$ for all g'_i on G_i and for all i. Hence (iv) is proved. (v) is an immediate consequence of our Lemma 7. Since $G=\bigcup_0^m G_i$ is normally algebraic over k, we see that $\sum Z_i$ remains unchanged by any automorphism of the universal domain over k, which proves (vi).

Let w_i be a point on W_i and assume that g_i, g'_i are two corresponding points on G_i. Let w_0 be a generic point of W_0 over $K(w_i, g_i, g'_i)$ and let g_0 be the corresponding point on G_0. Let Z_{0ii} be the subvariety of $W_0\times W_i\times W_i$ defined in our Lemma 7. Then by Lemam 7, (v) and (vi), $Z_{0ii}\cap(w_0\times w_i\times W_i)$ reduces to a point (w_0, w_i, v_i) and v_i is a generic point of W_i over K. Let h_i be the point on G_i corresponding to v_i. Then we see immediately that $g_i\cdot g_0=g'_i\cdot g_0=h_i$, which proves $g_i=g'_i$. Since $W_i\cap W_j=\emptyset$ whenever $i\neq j$, and since we have taken for G_i the graph of our normalization $W_i\to G'_i$, it follows that $G_i\cap G_j=\emptyset$ whenever $i\neq j$. Our statement (iii) follows now immediately.

COROLLARY 1. *Let A be a polarized abelian variety, polarized by a set $\mathfrak{X}$. Then $\mathfrak{G}(A,\mathfrak{X})$ is a finite group.*

Proof. Let V be a variety and Z be a subvariety of $V\times A\times A$ such that $Z(v)$ defined by $(v\times A\times A)\cdot Z=v\times Z(v)$ is the graph of an automorphism f_v of the underlying polarized variety of A. Let O be the neutral element of A and put $f_v(O)=O_v$. Then $f_v-O_v=\alpha$ is an automorphism of our polarized abelian variety A. Let k be an algebraically closed common field of definition for A, for V and for Z. Then since α is an automorphism of A defined over $k(v)$, we see that α is defined over k, by taking v to be a generic point of V over k (cf. Chow [2]). Therefore, when v' is a point on V such that $Z(v')$ is defined and is the graph of an automorphism of the underlying polarized variety of A, $f_{v'}-O_{v'}=\alpha$. Our corollary now follows immediately from our theorem.

COROLLARY 2. *Maintaining the same notations and assumptions as our theorem, G_0 is a normal subgroup of G. Denoting by $P(U)$ the Picard variety of U and by β the canonical homomorphism of $G_a(U)$ onto $P(U)$, there is a rational homomorphism F of G_0 into $P(U)$ defined by $F(g)=\beta(Z_0(g)^{-1}(X)-X)$ with a fixed U-divisor X. F depends only on the class of X with respect to algebraic equivalence. When we take X to be a linearly effective divisor on U, the kernel H_0 of F is a subgroup of a projective general linear group, and H_0 is a normal subgroup of G_0.*

Proof. Let K be a common field of definition for U, for every G_i, Z_i and for $P(U)$ and β. Since G_0 is a group variety of finite index in G, it follows that G_0 is a normal subgroup of G. Let X be a U-divisor and K' be a field containing K over which X is rational. Let g be a generic point of G_0 over K' and let F be the mapping of G_0 into $P(U)$ defined by

$$F(g)=\beta(Z_0(g)^{-1}(X)-X).$$

Then F is an everywhere defined rational mapping. F is then a rational homomorphism up to a constant (cf. Weil [17], no. 19). Since the neutral element e of G_0 is such that $Z_0(e)=\Delta$, it follows that F itself is a homomorphism. Let Y be another U-divisor such that $X\equiv Y \bmod G_a(U)$, and F' be the similar homomorphism defined in terms of Y. Since we have $Z_0(g')^{-1}(X-Y)\sim(X-Y)$ for any g' on G_0 by our Prop. 5, it follows that $F=F'$. Let us now assume that X is linearly effective. Then since the kernel H_0 of F consists of those g' such that $Z_0(g')^{-1}(X)\sim X$, it follows that H_0 can be identified with an algebraic subgroup of the group of projective transformations $PGL(m)$, where $m=l(X)-1$. Our corollary is thereby proved.

Let U be a non-singular projective variety and G be an abstract group of automorphisms of U. Then by Proposition 5 and Theorem 6, we see that *G contains the largest connected algebraic subgroup and to put a structure of polarization on U has an effect of cutting down the set of cosets with respect to the subgroup to a finite set.* The author found this when Weil pointed out that the original proof of our Corollary 1 can be generalized to our Theorem 6.

Section 4.

12. We shall define the field of moduli of a polarized variety (resp. abelian variety) V. Let $\mathfrak{P}(V,\mathfrak{X}^*)=\bigcup\mathfrak{P}(V,\mathfrak{A})$, where $\mathfrak{X}^*$ is the subset of $\mathfrak{X}$ defined in our Theorem 4. Then the *field of moduli* of V is the smallest field K with the following properties:

(i) One of the $\mathfrak{P}(V,\mathfrak{A})$ in the above expression for $\mathfrak{P}(V,\mathfrak{X}^*)$ is defined over K;

(ii) Every other $\mathfrak{P}(V,\mathfrak{A})$ in the above expression for $\mathfrak{P}(V,\mathfrak{X}^*)$ is defined over a separably generated extension of K.

We are going to prove some lemmas, which we shall need to prove the existence theorem.

LEMMA 8. *Let V be a complete non-singular variety (resp. abelian variety) and $\mathfrak{A}$, $\mathfrak{A}'$ be complete families of V-divisors consisting of algebraically effective positive divisors. Let K be a field of definition for $\mathfrak{P}(V,\mathfrak{A})$. Then $\mathfrak{P}(V,\mathfrak{A}')$ is defined over an algebraic extension of K.*

Proof. Without loss of generality, we may assume that K is algebraically closed. First let us assume that V is a complete non-singular variety, and X, Y be divisors in $\mathfrak{A}, \mathfrak{A}'$ respectively. Since K is algebraically closed, there is a variety V' contained in $\mathfrak{P}(V,\mathfrak{A})$, defined over K. There is an isomorphism f between V and V' such that $\mathfrak{A}$ is transformed to the complete algebraic family on V' containing a hyperplane section of V'. Also $\mathfrak{A}'$ is transformed to the complete algebraic family on V' containing $f(Y)$ by f. Since $\mathfrak{A}(f(Y))$ is a complete family and since K is algebraically closed, $\mathfrak{A}(f(Y))$ is defined over K. Since $\mathfrak{P}(V,\mathfrak{A}') = \mathfrak{P}(V',\mathfrak{A}(f(Y)))$, our lemma follows from Theorem 3 in this case. When V is an abelian variety, our lemma follows easily from the definitions and from what we have proved.

LEMMA 9. *Let V be a complete non-singular variety (resp. abelian variety) and X be a positive algebraically effective divisor. Assume that $\mathfrak{A}(X)$ and $\mathfrak{A}(mX)$ are complete total families of V-divisors, where m is a positive integer. Let K and K' be the smallest fields of definitions of $\mathfrak{P}(V,\mathfrak{A}(X))$ and $\mathfrak{P}(V,\mathfrak{A}(mX))$ respectively. Then K' is a subfield of K.*

Proof. Since $\mathfrak{P}(V,\mathfrak{A}(X))$ has a structure of an algebraic variety over K by Theorem 3, we can speak of a generic variety of $\mathfrak{P}(V,\mathfrak{A}(X))$ over K. Let V^* be a generic variety of it over K. There is an isomorphism f^* of V onto V^* such that $f^*(\mathfrak{A}(X))$ is a complete total family of V^*-divisors containing hyperplane sections of V^*. Hence $f^*(\mathfrak{A}(X))$ contains a rational divisor over any field of definition of the underlying variety of V^*. Let K^* be a regular extension of K, over which V^* is defined. Then since $f^*(\mathfrak{A}(X))$ contains a rational divisor over K^*, and since it is complete and total, it is defined over K^* (Matsusaka [6], Prop. 1). $f^*(\mathfrak{A}(mX))$ is the complete total family on V^* containing $f^*(mX)$ and hence it also contains a rational divisor over K^*. Therefore $f^*(\mathfrak{A}(mX))$ is also defined over K^*. Since $\mathfrak{P}(V,\mathfrak{A}(mX)) = \mathfrak{P}(V^*,f^*(\mathfrak{A}(mX)))$, it follows that $\mathfrak{P}(V,\mathfrak{A}(mX))$ is defined over K^*. On the other hand, $\mathfrak{P}(V,\mathfrak{A}(mX))$ is defined over an algebraic extension of K by Lemma 8, therefore it is defined over K and our lemma is thereby proved.

LEMMA 10. *Let U be a non-singular variety in a projective space and X be a positive U-divisor such that $\mathfrak{A}(X)$ and $\mathfrak{A}(mX)$ are total quasi-complete* *families consisting of algebraically effective divisors, where* m *is a positive integer. Let* K *be a common field of definition for* U *and* $\mathfrak{A}(mX)$*. If* m *is prime to the characteristic* p, $\mathfrak{A}(X)$ *is defined over a separably algebraic extension of* K.

Proof. In order to prove our lemma, we may identify K with its separably algebraic closure. Since every element in the algebraic closure $\bar{K}$ of K is purely inseparable over K, $\mathfrak{A}(X)$ has no other conjugate than itself over K since it is quasi-complete Let K' be a purely inseparable extension of K over which $\mathfrak{A}(X)$ is defined, and X^* be a generic divisor of $\mathfrak{A}(X)$ over K'. Without loss of generality, we may identify X^* with X. Let $K'(u)$ be the smallest field containing K' over which X is rational. There is a positive integer s such that $K(u^{p^s})$ is a regular extension of K, where u^{p^s} is the point whose coordinates are the p^s-th power of the coordinates of u. Also there is a positive integer t such that p^tX is rational over $K(u^{p^s})$. Since m and p^t are relatively prime, there are two integers a and b such that when Y is a generic divisor of $\mathfrak{A}(mX)$ over $K(u^{p^s})$, $aY + bp^tX \equiv X \bmod G_a(U)$. Moreover, $aY + bp^tX$ is rational over a regular extension of K by our choice of Y. We claim that $\mathfrak{L}^*(aY + bp^tX)$ contains a positive divisor. Since $aY + bp^tX - X$ is algebraically equivalent to 0, there is a positive divisor X' in $\mathfrak{A}(X)$ such that $aY + bp^tX - X \sim X' - X$. Therefore, $\mathfrak{L}^*(aY + bp^tX)$ contains a positive divisor, and we may assume that X' is rational over the same regular extension of K over which $aY + bp^tX$ is rational (cf. Weil [16], Chap. VIII, Cor. 1, Th. 10). Since $\mathfrak{A}(X)$ contains a rational divisor X' over a regular extension of K, and since it is quasi-complete total family, $\mathfrak{A}(X)$ is defined over a regular extension of K (Matsusaka [6], Prop. 1). Therefore $\mathfrak{A}(X)$ must be defined over K and our lemma follows now from Theorem 3.

13.

THEOREM 7. *Let* V *be a complete non-singular variety (resp. abelian variety), polarized by a set* $\mathfrak{X}$ *and assume either that the order of* $G_n(V)/G_a(V)$ *is prime to the characteristic* p *or isomorphisms between* V', V'' *in* $\mathfrak{P}(V, \mathfrak{X})$ *are defined over separably generated extensions of any common field of definition for* V', V''*. Then there is the field of moduli of* V*. When the characteristic is* 0, *it has the additional property that any field of definition of* $\mathfrak{P}(V, \mathfrak{A})$*, which appears in the expression for* $\mathfrak{P}(V, \mathfrak{X}^*)$*, contains the field of moduli.*

Proof. Let r be the order of $G_n(V)/G_a(V)$. By Proposition 4, there is the divisor class $\mathfrak{N}^*$ on V with respect to $G_n(V)$ such that X belongs to $\mathfrak{X}$ if and only if X is positive and belongs to $m\mathfrak{N}^*$ for a certain positive integer m. There is a positive integer m_0 such that whenever $m' > m_0$, $m'\mathfrak{N}$ is not empty, contains a numerically effective divisor and is covered exactly by r complete total families (cf. Th. 1). Let us fix an integer m' with that property. Let $m'\mathfrak{N}$ be covered by complete total families $\mathfrak{A}(X_i)$. Let us denote by k_i the smallest field of definition of $\mathfrak{P}(V, \mathfrak{A}(X_i))$. Put $K^* = k_1 \cup \cdots \cup k_r$ and let $k_{i,m}$ be the smallest field of definition for $\mathfrak{P}(V, \mathfrak{A}(mX_i))$, where m is a positive integer. We shall show that K^* contains $k_{i,m}$ and is a finite normal extension of the latter, satisfying $[K^* : k_{i,m}]_s \leqq r$.

By Lemma 9, k_i contains $k_{i,m}$ and the former is an algebraic extension of the latter by Lemma 8. Since there is a positive integer a such that aX_i and aX_j are algebraically equivalent to each other on V, and since $\mathfrak{A}(aX_i)$ is a complete total family consisting of numerically effective divisors by our choice of m', k_j is an algebraic extension of $k_{i,a}$, again by Lemmas 8 and 9. If we take a to be a multiple of m, $k_{i,m}$ itself is an algebraic extension of $k_{i,a}$ and consequently $k_i \cup k_j$ is an algebraic extension of $k_{i,m}$ for every j. Thus we have shown that K^* contains $k_{i,m}$ and is an algebraic extension of $k_{i,m}$. Let k_0 be the prime field and let W_i be the open algebraic variety, which is the set of points $c(f(V))$, where f is a non-degenerate projective embedding determined by a divisor in $\mathfrak{A}(X_i)$ (cf. Th. 3). Let (w_i) be a set of quantities such that $k_0((w_i)) = k_i$. Let U_i be a generic variety of $\mathfrak{P}(V, \mathfrak{A}(mX_i))$ over k_i and $k_{i,m}(u_i)$ be the smallest field of definition for U_i containing $k_{i,m}$. There is an isomorphism between V and U_i, say f_i, such that $f_i(\mathfrak{A}(mX_i))$ is the complete total family of U_i-divisors containing hyperplane sections of U_i, and we have clearly $\mathfrak{P}(V, \mathfrak{A}(X_j)) = \mathfrak{P}(U_i, f_i(\mathfrak{A}(X_j)))$. Let α be an automorphism of the universal domain over $k_{i,m}(u_i)$. We have $U_i^\alpha = U_i$, $(f_i(\mathfrak{A}(X_j)))^\alpha = \mathfrak{A}((f_i(X_j))^\alpha)$. Therefore $k_{i,m}((w_j)^\alpha)$ is the smallest field of definition for $\mathfrak{P}(U_i, \mathfrak{A}((f_i(X_j))^\alpha))$. Since $f_i(\mathfrak{A}(mX_i))$ contains a rational divisor over $k_{i,m}(u_i)$, it follows that $f_i(X_j)^\alpha \equiv f_i(X_i) \bmod G_n(V)$ and this shows that $k_{i,m}((w_j)^\alpha)$ coincides with one of the $k_{i,m}((w_j))$. Since $K^* = k_{i,m}((w_1), \cdots, (w_r))$, it follows that K^* is a normal extension of $k_{i,m}$ and $[K^* : k_{i,m}]_s \leqq r$.

Let $k'_{i,m}$ be the largest purely inseparable extension of $k_{i,m}$ in K^*. When t is a positive integer, we have $k_{i,m} \supset k_{i,tm}$ by Lemma 9 and $k'_{i,tm}$ is the smallest subfield of K^* containing $k_{i,tm}$ over which K^* is a separably algebraic extension. Therefore, we have $k'_{i,m} \supset k'_{i,tm}$ and $[K^* : k'_{i,tm}] \leqq r$. From this we see that there is a positive integer t_0 such that whenever $t > t_0$, we have $k'_{i,t_0m} = k'_{i,tm}$. Let us take m and m' to be prime to the characteristic p (this is certainly possible because of our Theorem 1) and put

$$K = k'_{i,t_0m}.$$

We are going to show that K is the field we are looking for. Let $\mathfrak{P}(V, \mathfrak{A}(Y))$ be a component of $\mathfrak{P}(V, \mathfrak{X}^*)$ and (y) be a set of quantities such that $k_0((y))$ is the smallest field of definition for $\mathfrak{P}(V, \mathfrak{A}(Y))$. Y is contained in $s\mathfrak{N}^*$ for a suitable choice of s by Proposition 4. Let t be a positive integer prime to the characteristic p. Then $b = tmm'$ is prime to p and $\mathfrak{N}(bsX_i) = \mathfrak{N}(bm'Y)$. Moreover, we have $K = k'_{i,bs}$. Let U be a generic variety of $\mathfrak{P}(V, \mathfrak{A}(bsX_i))$ over K, then it is still a generic variety of it over K^* and there is an isomorphism g between V and U such that $g(\mathfrak{A}(bsX_i))$ is the complete total family on U, containing hyperplane sections of it. Let $K(u)$ be the smallest field of definition for U containing K, which is a regular extension of K by Theorem 3. Then since $g(\mathfrak{A}(bsX_i))$ contains a rational divisor over $K(u)$, it is defined over $K(u)$ (cf. Matsusaka [6], Prop. 1).

Assume for a moment that $G_n(U)/G_a(U)$ has a set of representatives in $G_n(U)$ which consists of divisors rational over a separably generated extension of $K(u)$. Then $\mathfrak{N}(bsX_i)$ is covered by r complete total families consisting of numerically effective divisors by our choice of m' and each family is defined over a separably generated extension of $K(u)$ (cf. Matsusaka [6], Prop. 1), and consequently over a separably algebraic extension of $K(u)$. Therefore $\mathfrak{A}(g(bm'Y))$ on U is defined over a separably algebraic extension of $K(u)$ and since b and m' are prime to p, it follows that $\mathfrak{A}(g(Y))$ itself is defined over a separably algebraic extension of $K(u)$ by Lemma 10. This implies that $\mathfrak{P}(U, \mathfrak{A}(g(Y)))$ is defined over a separably algebraic extension of $K(u)$ by Theorem 3; since $\mathfrak{P}(V, \mathfrak{A}(Y)) = \mathfrak{P}(U, \mathfrak{A}(g(Y)))$, our field K satisfies our requirements (i) and (ii). Let us prove now that K is the smallest field having the properties (i) and (ii). Let K' be any field satisfying (i) and (ii). By Lemma 8 and by the definition of K^*, $K^* \cup K'$ is a separably algebraic extension of K'. By (i), there is a component $\mathfrak{P}(V, \mathfrak{A}(Y))$ of $\mathfrak{P}(V, \mathfrak{X}^*)$ such that it is defined over K'. There are two positive integers b and c such that $\mathfrak{A}(bX_i) = \mathfrak{A}(cY)$ and we may take b to be a multiple of t_0m. Then $k_{i,b}$ is the smallest field of definition for $\mathfrak{P}(V, \mathfrak{A}(cY))$, which is a subfield of K' by Lemma 9. By our choice of b, we have $k_{i,b} \subset k'_{i,b} = K$. It follows that K is a purely inseparable extension of $K \cap K'$. Let d be any element of K, then d is purely inseparable over K' and is contained in $K^* \cup K'$. Since $K^* \cup K'$ is separably algebraic over K', d must be in K', which proves that K is a subfield of K'.

Now let us prove that $G_n(U)/G_a(U)$ has a set of representatives in $G_n(U)$ which consists of divisors, rational over a separably generated extension of $K(u)$. First assume that r is prime to p. Put $Z=g(bsX_i)$, then $\mathfrak{R}(Z)$ contains a rational divisor over $K(u)$, i.e. a hyperplane section of U, and is covered by r distinct complete total families. Let $\mathfrak{A}_1,\cdots,\mathfrak{A}_r$ be such and assume that Z is contained in $\mathfrak{A}_1$. Then $\mathfrak{A}_1$ is defined over $K(u)$ since it is our $g(\mathfrak{A}(bsX_i))$. Since $r\mathfrak{A}_1=r\mathfrak{A}_i$, $r\mathfrak{A}_i$ is also defined over $K(u)$ and hence $\mathfrak{A}_i$ is defined over a separably algebraic extension of $K(u)$ by Lemma 10. Therefore $\mathfrak{A}_i$ contains a divisor which is rational over a separably algebraic extension of $K(u)$. Our assertion is proved in this case. Next assume that isomorphisms between V', V'' in $\mathfrak{P}(V,\mathfrak{X}^*)$ are defined over separably generated extensions of any common field of definition for V', V''. Let $U_1,\cdots,U_r$ be independent generic varieties of $\mathfrak{P}(V,\mathfrak{A}(X_1)),\cdots,\mathfrak{P}(V,\mathfrak{A}(X_r))$ over $K^*(u)$. There is a regular extension $K^*(u,w)$ of $K^*(u)$ over which every U_i is defined. Let g, f_i be isomorphisms between V and U, V and U_i respectively. Then $g\cdot f_i^{-1}$ is an isomorphism between U_i and U which is defined over a separably generated extension of $K^*(u,w)$ by our assumption. $\mathfrak{A}(f_i(X_i))$ is defined over $K^*(u,w)$ and since we have $g(X_i)=g\cdot f_i^{-1}(f_i(X_i))$, $\mathfrak{A}(g(X_i))$ is defined over a separably generated extension of $K^*(u,w)$. Hence $\mathfrak{A}(g(X_i))$ contains a divisor which is rational over a separably generated extension of $K^*(u,w)$ and our assertion is proved also in this case.

When $p=0$, the second condition about the field of moduli is automatically satisfied. Therefore, K is the smallest field over which one of components of $\mathfrak{P}(V,\mathfrak{X}^*)$ is defined. Our theorem is thereby proved completely.

Assumptions in our theorem are satisfied when $p=0$, or when V is a polarized abelian variety (cf. Chow [2]). Hence in these cases, there exist fields of moduli.

14. Let U be an algebraic variety and $G=\{f_i\}$, $0\leqq i\leqq r$, be a finite group of automorphisms of U. *The quotient variety of U with respect to G* is, by definition, the following pair (W,ϕ) of a variety W and a rational mapping ϕ of U onto W:

(i) ϕ is defined everywhere on U;

(ii) $\phi=\phi\cdot f_i$ for all i;

(iii) When ϕ' is a rational mapping of U onto a variety W' with $\phi'=\phi'\cdot f_i$ for all i, then $\phi'=\psi\cdot\phi$, where ψ is a rational mapping of W onto W' such that when ϕ' is defined at u' on U, ψ is defined at $\phi(u')$.

Sometimes ϕ is called the *canonical mapping* of U onto W. (W,ϕ) is clearly defined uniquely up to an isomorphism when it exists. When U is a projective variety, the existence has been proved by Serre (cf. J. P. Serre [12], § 3, no. 13). Moreover, when that is so, W can be realized as a projective variety; when U is defined over a field k, the f_i are defined over a separably algebraic extension of k and $f_i^\alpha = f_j \in G$ whenever α is an automorphism of the universal domain over k, then there is a quotient variety (W,ϕ) such that W and ϕ are defined over k. Let now A be a polarized abelian variety, polarized by a set of divisors $\mathfrak{X}$. By Corollary 1, Theorem 6, $\mathfrak{G}(A,\mathfrak{X})$ is a finite group and when k is a field of defintion for A, every automorphism in $\mathfrak{G}(A,\mathfrak{X})$ is defined over a separably algebraic extension of k (cf. Chow [2]). Hence there is a quotient variety (W,ϕ) of A with respect to $\mathfrak{G}(A,\mathfrak{X})$ such that W,ϕ are defined over k and that W is a projective variety. In general, the quotient variety (W,ϕ) of A with respect to $\mathfrak{G}(A,\mathfrak{X})$ shall be called a *generalized Kummer variety* of the polarized abelian variety A. When the ring of endomorphisms of A is isomorphic to the ring of integers, $\mathfrak{G}(A,\mathfrak{X})$ consists of two elements and in this case our generalized Kummer variety coincides with the usual Kummer variety of A. It is easy to see that any generalized Kummer variety is such that its Albanese variety reduces to a point.

THEOREM 8. *Let V be a polarized variety (resp. polarized abelian variety), polarized by a set $\mathfrak{X}$ and assume that there exists the field of moduli. Assume the following:*

(a) *$\mathfrak{G}(V,\mathfrak{X})$ is a finite group;*

(b) *For any pair (U,U') of elements in $\mathfrak{P}(V,\mathfrak{X})$ and for any choice of a common field of definition K' for U and U', isomorphisms between U and U' are defined over separably generated extensions of K'.*

Let K be the field of moduli of V, then to each U in $\mathfrak{P}(V,\mathfrak{X})$, there is a quotient variety (W,ϕ_U) of U with respect to the group of automorphisms of the polarized U with the following properties:

(i) *W is defined over K and is independent of U;*

(ii) *ϕ_U is defined over the smallest field of definition for U containing K;*

(iii) *When U and U' are any two elements in $\mathfrak{P}(V,\mathfrak{X})$ and $f_{U',U}$ is an isomorphism of U to U', then $\phi_{U'} = \phi_U \cdot f_{U',U}^{-1}$.*

(Remark: When V is a polarized abelian variety, (a) and (b) are automatically satisfied (cf. our Cor. 1; Th. 6; Weil [17], Th. 6; Chow [2])).

Proof. Let U_1 and U_2 be elements of $\mathfrak{P}(V, \mathfrak{X})$ and k_1, k_2 be the smallest fields of definitions for U_1, U_2 respectively. Let the (W_i, ϕ_i) be quotient varieties of the U_i with respect to the groups of automorphisms $\mathfrak{G}(U_i)$ of U_i. We shall show that there is an isomorphism $\psi_{2,1}$ of W_1 and W_2 such that $\phi_2 \cdot f_{2,1} = \psi_{2,1} \cdot \phi_1$ for any isomorphism $f_{2,1}$ of U_1 to U_2, and that when k' is a common field of definition for W_1, ϕ_1, W_2 and ϕ_2, $\psi_{2,1}$ is defined over k'. It is easy to see that our two groups $\mathfrak{G}(U_1)$ and $\mathfrak{G}(U_2)$ are isomorphic by the correspondence $f_j^{(1)} \rightarrow f_{2,1} \cdot f_j^{(1)} \cdot f_{2,1}^{-1}$, where the $f_j^{(1)}$ are elements of $\mathfrak{G}(U_1)$. Moreover, every isomorphism between U_1 and U_2 can be written as $f_{2,1} \cdot f_j^{(1)}$. This shows in particular that the set of isomorphisms between U_1 and U_2 is finite by (a). Let x be a generic point of U_1 over k'. We claim that the mapping $\psi_{2,1}$ defined by $\phi_1(x) \rightarrow \phi_2(f_{2,1}(x))$ satisfies all our requirements. In fact, since $f_{2,1} \cdot f_j^{(1)}$ can be written as $f_i^{(2)} \cdot f_{2,1}$, where $f_i^{(2)}$ is an element of $\mathfrak{G}(U_2)$, we see that

$$\phi_2(f_{2,1}(f_j^{(1)}(x))) = \phi_2(f_i^{(2)}(f_{2,1}(x))) = \phi_2(f_{2,1}(x)).$$

Hence our assertion is proved.

By Theorem 7, there is a component $\mathfrak{A}$ of $\mathfrak{X}^*$ such that $\mathfrak{P}(V, \mathfrak{A})$ is defined over the field of moduli K. By our definition of $\mathfrak{X}^*$, $\mathfrak{A}$ is a complete total family consisting of algebraically effective divisors. Let U_u and U_v be two independent generic elements of $\mathfrak{P}(V, \mathfrak{A})$ over K such that $K(u)$ and $K(v)$ be the smallest fields of definitions for U_u and for U_v containing K (cf. Th. 3). Then $K(u)$ and $K(v)$ are regular extensions of K such that they are linearly disjoint over K. Then there exist quotient varieties $(W_u, \bar{\phi}_u)$, $(W_v, \bar{\phi}_v)$ of U_u, U_v with respect to the groups of automorphisms $\mathfrak{G}(U_u)$, $\mathfrak{G}(U_v)$ of polarized varieties U_u, U_v, defined over $K(u), K(v)$ respectively by our assumptions (a) and (b). By what we have observed, there is an isomorphism $\psi_{u,v}$ of W_u to W_v defined over $K(u, v)$ such that $\bar{\phi}_v \cdot f_{v,u} = \psi_{v,u} \cdot \bar{\phi}_u$, for any isomorphism $f_{v,u}$ between U_u and U_v. Let now u, v and w be three independent generic specializations of u over K. Then we see easily that $\psi_{w,v} \cdot \psi_{v,u} = \psi_{w,u}$. Since U_u, U_v, U_w are projective varieties, we may assume that W_u, W_v, W_w are again projective varieties. Therefore, there is a variety W in a projective space defined over K and the isomorphism h_u between W_u and W defined over $K(u)$ such that $\psi_{v,u} = h_v^{-1} \cdot h_u$ (cf. Weil [21], Th. 5). Put $\phi_u = h_u \cdot \bar{\phi}_u$. Clearly, (W, ϕ_u) is also a quotient variety of U_u with respect to $\mathfrak{G}(U_u)$. Moreover, for any isomorphism $f_{v,u}$ of U_u to U_v, we have $\phi_v \cdot f_{v,u} = \phi_u$.

Let U' be any element of $\mathfrak{P}(V,\mathfrak{X})$ and $(W',\bar{\phi}')$ be a quotient variety of U' with respect to $\mathfrak{G}(U')$. By what we have seen in the beginning of our proof, there is an isomorphism ψ' between W and W' such that, for any isomorphism f_v' of U_v to U', we have $\bar{\phi}'\cdot f_v'=\psi'\cdot\phi_v$. Hence if we put $\phi'=\psi'^{-1}\cdot\bar{\phi}'$, (W,ϕ') is a quotient variety of U' and satisfies (i) and (iii). Let K' be the smallest field of definition for U' containing K. By (b), we may then assume that $(W',\bar{\phi}')$ is defined over K'. By the definition of ϕ', $\phi'=\phi_v\cdot f_v'^{-1}$ for any isomorphism f_v' of U_v and U'. Therefore ϕ' is defined over $K'(v)$ by our assumption (b). Since we can write also $\phi'=\phi_u\cdot f_u'^{-1}$ for any isomorphism f_u' of U_u and U', ϕ' is also defined over $K'(u)$ and this proves that K' is a field of definition for ϕ'. Our theorem is thereby proved.

THE UNIVERSITY OF CHICAGO, AND
NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] N. Bourbaki, "Théorie des ensembles," *Actualités Scientifiques et Industrielles*, No. 846 (1951).

[2] W. L. Chow, "Abelian varieties over function fields," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 253-275.

[3] ———, "Abstract theory of the Picard and Albanese varieties," to appear.

[4] ——— and B. L. van der Waerden, "Zur Algebraischen Geometrie IX," *Mathematische Annalen*, vol. 113 (1937), pp. 692-794.

[5] T. Matsusaka, "On the algebraic construction of the Picard variety," *Japanese Journal of Mathematics*, vol. 21 (1951), pp. 217-235.

[6] ———, "On the algebraic construction of the Picard variety II," *ibid.*, vol. 22 (1952), pp. 51-62.

[7] ———, "On the algebraic families of positive divisors," *Journal of the Mathematical Society of Japan*, vol. 5 (1953), pp. 115-136.

[8] ———, "Some theorems on abelian varieties," *Natural Science Report*, Ochanomizu University, vol. 4 (1953), pp. 22-25.

[9] ———, "The criteria for algebraic equivalence and the torsion group," *American Journal of Mathematics*, vol. 79 (1957), pp. 53-66.

[10] A. Néron, "Problèmes arithmétiques et géométriques rattachés a la notion du rang d'une courbe algébriques dans un corps," *Bulletin de la Société Mathématique de France*, vol. 80 (1952), pp. 101-166.

[11] ——— and P. Samuel, "La variété de Picard d'une variété Normale," *Annales de l'institut Fourier*, vol. 4 (1952), pp. 1-30.

[12] J. P. Serre, "Sur la topologie des variétés algébriques en caractéristique p," *Symposium de topologie algébrique*, Mexico, 1956, to appear.

[13] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[14] C. L. Siegel, "Lectures on the analytic theory of quadratic forms," Princeton lecture note, revised edition (1949).

[15] B. L. van der Waerden, *Einführung in die algebraische Geometrie*, Berlin (1939).

[16] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society, Colloquium Publication, vol. 29 (1946).

[17] ———, "Variétés Abéliennes et Courbes Algébriques," *Actualités Scientifiques et Industrielles*, No. 1064 (1948).

[18] ———, "Sur les critères d'équivalence en géométrie algébrique," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[19] ———, "Projective embeddings of abelian varieties," Algebraic Geometry and Topology (A symposium in honor of S. Lefschetz), pp. 177-181.

[20] ———, "On algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955), pp. 355-391.

[21] ———, "The field of definition of a variety," *ibid.*, vol. 78 (1956), pp. 509-524.

[22] ———, "On the theory of complex multiplication," *Proceedings of the International symposium on Algebraic Number Theory* (1955), pp. 9-22.

[23] O. Zariski, "Foundations of a general theory of birational correspondences," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 490-542.

CONFORMAL INVARIANTS AND PRIME ENDS.*[1]

By Ernest C. Schlesinger.

Introduction. From the point of view of conformal mapping, it is unsatisfactory to consider the individual points of the boundary of a simply connected region as the primitive constituents of this boundary. When such a region is mapped conformally onto the unit disk, in accordance with the Riemann mapping theorem, the points of the unit circumference correspond, indeed, to the prime ends of the region. These prime ends are here considered as equivalence classes of sequences of points of the region under a relation P^*. The principal tool we employ to introduce this relation is extremal length, a conformally invariant quantity associated with a family of curves. Its definition was first given by Ahlfors and Beurling ([2], [3]).

The term "prime end" originated with Carathéodory [4], who initiated the systematic study of the structure of the boundary of a simply connected region. His approach was topological, and it dealt with concepts—subregions, crosscuts, etc.—which are defined with reference to the given region. It is easily seen that with Carathéodory's definition the prime ends of the unit disk correspond to points on the circumference in the sense that an equivalence class is associated with each boundary point and that two sequences belong to the same class if and only if they converge to the same point of the circumference. The problem that arises under his approach, however, and this is solved by one of Carathéodory's fundamental theorems, is that one must show that prime ends are preserved under conformal mapping.

Lindelöf [6] circumvented this difficulty by defining prime ends by reference to the conformal map of the disk onto the region; namely in terms of the set of indetermination or cluster set. However, his method does not obviate an explicit analysis of the topological situation in the region itself. Lindelöf also obtained the following result, which is related to the classification of prime ends.

Carathéodory had distinguished two classes of points, principal and subsidiary (see Section 2.7, below), on the point set of a prime end, i. e. on the

---

* Received July 11, 1957; revised December 2, 1957.

[1] This paper is a revision of part of the author's dissertation (Harvard University, 1955). Part of the research was carried on under support from ONR Contract No. NR-ori-07634 with Harvard University.

set of accumulation points of all sequences belonging to the prime end. Lindelöf showed that if a sequence of points of the disk converges to a boundary point in an angle (non-tangentially) then the image sequence has only principal points of the corresponding prime end for accumulation points. This is a precise way of stating that the principal points form a kind of nucleus for the point set of the prime end.

Two other schemes for defining prime ends deserve brief mention. Mazurkiewicz [7] introduced a metric, $\rho_\pi(z_1, z_2)$, equivalent to the euclidean metric in the region in the sense that $\rho_\pi(z_j, z_0) \to 0$ if and only if $| z_j - z_0 | \to 0$ for any sequence $\{z_j\}_1^\infty$ of points of the region. The boundary of the region with respect to ρ_π (i. e. the complement of the region with respect to its ρ_π-completion) is a space which can be identified with the set of prime ends of Carathéodory.

Ursell and Young [9] have used the notion of an equivalence class of paths, which converge to the boundary of the region, to introduce the prime ends of the region.

The purpose of the present paper is to define prime ends once more. We use extremal length, and thus, we are able to give our definition in terms of constructs related to the region itself, while we obtain the conformally invariant nature of our prime ends immediately, since extremal length is a conformally invariant quantity. Finally, we state and prove in a conformally invariant form the theorem of Lindelöf, relating to approach in an angle, to which we referred above. For this purpose we attach a conformal invariant (an extremal length) to each point of a sequence which converges to a prime end. Our condition is then formulated in terms of the boundedness of the sequence of conformal invariants.

The author takes this opportunity to express his particular gratitude to Professor Lars V. Ahlfors of Harvard University who suggested the problem and whose encouragement and guidance at every stage made the completion of the study possible.

I. Extremal Length.

1. 0 Summary. Our principal tool is extremal length, a conformally invariant quantity associated with a family of curves. In this section, we first make precise the special meaning of some of the terms used in the sequel. Then we give the definition of extremal length, and state, partly without proof, those of its properties which are needed for our investigation.

1.1 All our point sets are assumed to lie on the Riemann sphere, which we denote by Σ. The spherical distance, $\psi(z,w)$, of the points with coordinates z and w, is used throughout.

A region, as always, is an open connected subset of Σ; it is simply connected if its complement with respect to Σ is connected. The closure and boundary of a region Ω are denoted by $\bar{\Omega}$ and $bd\,\Omega$, respectively. A configuration consists of a region and a set of distinguished points of the closure of the region. This set may contain interior points, isolated boundary points, or sub-continua of the boundary of the region.

Let Ω be a region. An arc of Ω shall be a continuous map, $z = z_\gamma(t)$, of an (open, half-open, or closed) interval into Ω. We denote the map and the point set of the arc, i. e. the subset of the region Ω onto which the interval is mapped, by the same symbol γ; when we want to emphasize that we are dealing with the point set, we shall occasionally use (γ). A closed arc of Ω is the continuous map of a closed interval into Ω for which the images of the initial and terminal points coincide. An arc γ is simple, if $z_\gamma(t_1) = z_\gamma(t_2)$ only if $t_1 = t_2$, or (in case of a closed arc) if t_1 and t_2 are endpoints of the parameter interval.

We shall also consider certain finite collections of arcs of Ω; such a collection of arcs we shall call a *generalized curve.*

An arc γ of Ω will be called a *crosscut of* Ω, provided its point set, (γ), is the homeomorph of an open interval, and $\Omega - (\gamma)$ has precisely two components.[2] When we consider, in the sense of the preceding paragraph, generalized curves whose constituent arcs are crosscuts, we shall insist that the corresponding point set be connected. Thus we have the following definition.

DEFINITION 1. *A generalized crosscut of* Ω *is a finite collection* τ *of crosscuts* $\gamma_1, \gamma_2, \cdots, \gamma_n$ *of* Ω, *such that the point set* $(\tau) = \bigcup_{j=1}^{n} (\gamma_j)$ *is connected.*

1.2 Let Ω be a region, $\{\gamma\}$ a family of generalized curves of Ω, and let $\rho(z)$ be a non-negative real-valued function defined on Ω. If $\rho^2(z)$ is integrable over Ω, we set $A_\Omega(\rho) = A(\rho) = \int\int_\Omega \rho^2(z)\,dxdy \quad (z = x + iy)$, and otherwise, $A_\Omega(\rho) = \infty$.

---

[2] This is a modification of the classical definition, according to which the point set of a crosscut is the homeomorph of an open interval with the additional property that this homeomorphism is the restriction of a continuous map of the closure of the interval into the closure of the region, and that the endpoints of the interval correspond to points on the boundary of the region. It is well known that these classical crosscuts have the separating property demanded above ([5]; p. 106). However, this formulation of the notion of a crosscut does not yield a conformally invariant concept.

Let γ be a curve of the family $\{\gamma\}$. If there is a finite or countable sequence $\{\gamma_i\}$ of disjoint rectifiable arcs, which are parameterized by their arc lengths (i. e. the arc γ_i is given by $z = z_i(s_i)$, where $0 \leqq s_i \leqq l_i$, and l_i is the length of γ_i), such that $(\gamma) = \bigcup_1^\infty (\gamma_i)$, and if the integrals appearing in the following sum exist in the sense of Lebesgue, we set

$$l_\rho(\gamma) = \sum_{i=1}^{\infty} \int_{\gamma_i} \rho(z_i(s_i))\,ds_i.$$

If γ cannot be represented in the above fashion, we set $l_\rho(\gamma) = \infty$. Finally, we introduce the quantity

$$L(\rho) = L_{\{\gamma\}}(\rho) = \inf_{\gamma \in \{\gamma\}} l_\rho(\gamma),$$

where we agree that $L_{\{\gamma\}}(\rho) = \infty$ in case the family $\{\gamma\}$ is empty.

1. 3 Extremal length. The function $\rho(z)$ shall be called *admissible* (with respect to Ω and $\{\gamma\}$) if $A(\rho)$ and $L(\rho)$ are not both zero or both infinite.

DEFINITION 2. ([2], [3], [8]) *The quantity*

$$\lambda_\Omega(\gamma) = \lambda(\gamma) = \sup L^2(\rho)/A(\rho),$$

where the supremum is taken over all admissible functions $\rho(z)$, *is called the extremal length of the family of curves* $\{\gamma\}$ *with respect to the region* Ω.

The following observations are found in the literature. (For example: [1], [8].)

(a) Extremal length is a conformal invariant.

(b) The extremal length $\lambda_\Omega(\gamma)$ depends only on the carrier of the family of curves $\{\gamma\}$ and not on the remainder of the region Ω.

(c) Since the ratio $L^2(\rho)/A(\rho)$ is homogeneous of degree 0 in ρ, we can introduce certain normalizations in the class of admissible functions:

(i) Under the additional restriction that $\lambda(\gamma) < \infty$, we have $\lambda(\gamma) = \sup L_{\{\gamma\}}{}^2(\rho)$, where the supremum is now taken over all admissible functions ρ for which $A(\rho) = 1$.

(ii) If $\lambda(\gamma) > 0$, we have $\lambda^{-1}(\gamma) = \inf A(\rho)$, with the infimum taken over admissible ρ for which $L_{\{\gamma\}}(\rho) \geqq 1$.

(iii) In case $0 < \lambda(\gamma) < \infty$, we may take $\lambda(\gamma) = \sup L_{\{\gamma\}}(\rho)$, the supremum being taken over all admissible functions ρ which satisfy the condition $L_{\{\gamma\}}(\rho) = A(\rho)$.

1.4 The comparison principle. The following lemma and its corollary allow us to give simple estimates for the extremal length. The proof is included as a typical one.

LEMMA 1. *Let $\{\gamma\}$ and $\{\gamma'\}$ be two families of generalized curves of a region Ω such that each $\gamma \in \{\gamma\}$ contains a $\gamma' \in \{\gamma'\}$. Then $\lambda(\gamma) \geqq \lambda(\gamma')$.*

Proof. Let $\epsilon > 0$ be given and let $\rho'(z)$ be admissible for the family $\{\gamma'\}$, subject to the condition that

$$L_{\{\gamma'\}}{}^2(\rho')/A(\rho') > \lambda(\gamma') - \epsilon. \tag{1}$$

We define a function $\rho_0(z)$ in Ω by

$\rho_0(z) = \rho'(z)$ if z belongs to some γ', $\rho_0(z) = 0$ otherwise.

For $\gamma \in \{\gamma\}$, let γ' be one of the elements of $\{\gamma'\}$ contained in γ. Then

$$l\rho_0(\gamma) \geqq L_{\{\gamma'\}}(\rho'), \tag{2}$$

since either $l\rho_0(\gamma) = \infty$, or

$$l\rho_0(\gamma) = \int_\gamma \rho_0\, ds \geqq \int_{\gamma'} \rho'\, ds = l\rho'(\gamma') \geqq L_{\{\gamma'\}}(\rho').$$

Formula (2) holds for each $\gamma \in \{\gamma\}$, so that

$$L_{\{\gamma\}}(\rho_0) \geqq L_{\{\gamma'\}}(\rho'). \tag{3}$$

Also, it is clear that

$$A(\rho_0) \leqq A(\rho'). \tag{4}$$

We must show that ρ_0 is admissible for the family $\{\gamma\}$. Since the lemma holds trivially if $\lambda(\gamma') = 0$, we may assume that $A(\rho') < \infty$, and a fortiori $A(\rho_0) < \infty$. If $A(\rho_0) = 0$, then either (i) $A(\rho') = 0$, or (ii) $A(\rho') > 0$. In case (i), $L_{\{\gamma'\}}(\rho') > 0$, since ρ' is admissible for $\{\gamma'\}$, while in case (ii), we choose ϵ so that $0 < \epsilon < \lambda(\gamma')$ in (1), and we conclude from that formula that $L_{\{\gamma'\}}(\rho') > 0$. In either case, therefore, $A(\rho_0) = 0$ implies, by (3), that $L_{\{\gamma\}}(\rho_0) > 0$; hence, ρ_0 is admissible for $\{\gamma\}$. From formulas (3) and (4), we obtain

$$L_{\{\gamma\}}{}^2(\rho_0)/A(\rho_0) \geqq L_{\{\gamma'\}}{}^2(\rho')/A(\rho'),$$

and therefore, by (1), $\lambda(\gamma) > \lambda(\gamma') - \epsilon$. This holds for each positive ϵ, and consequently, $\lambda(\gamma) \geqq \lambda(\gamma')$.

COROLLARY. *In particular, if* $\{\gamma\}$ *is contained in* $\{\gamma'\}$, *then* $\lambda(\gamma) \geqq \lambda(\gamma')$.

1.5 For the following two configurations we can compute extremal lengths explicitly. (For proofs see [1] or [8].)

(a) Let Ω be the interior of a rectangle with sides of lengths a and b, and let $\{\gamma\}$ be the family of crosscuts of Ω which connect the two sides of length a. Then $\lambda(\gamma) = b/a$.

(b) Let Ω be the interior of the annulus formed by two concentric circles of radii r and $R (r < R)$. The family $\{\gamma\}$ of crosscuts of Ω which connect the two circles has extremal length $\lambda(\gamma) = \frac{1}{2\pi} \log(R/r)$, while the family $\{\gamma^*\}$ of simple closed arcs of Ω which separate the two boundary components has extremal length $\lambda(\gamma^*) = 2\pi/\log(R/r)$.

1.6 The next result allows us to conclude that if the union of two families of curves has vanishing extremal length, the same is true of at least one of these two families.

LEMMA 2. *If* $\{\gamma'\}$ *and* $\{\gamma''\}$ *are two non-empty families of generalized curves of a region* Ω, *and* $\{\gamma^0\}$ *is the union of these two families, then* $\lambda(\gamma') > 0$ *and* $\lambda(\gamma^0) = 0$ *imply that* $\lambda(\gamma'') = 0$.

Proof. [8; Satz 5] Assume $\lambda(\gamma'') > 0$, and let ρ' and ρ'' be admissible for the families $\{\gamma'\}$ and $\{\gamma''\}$, respectively; we normalize by the conditions that $L_{\{\gamma'\}}(\rho') \geqq 1$ and $L_{\{\gamma''\}}(\rho'') \geqq 1$. Set $\rho_0(z) = \max\{\rho'(z), \rho''(z)\}$. It is clear that $L_{\{\gamma^0\}}(\rho_0) \geqq 1$, and $A(\rho_0) \leqq A(\rho') + A(\rho'')$. Hence, the function ρ_0 is admissible for the family $\{\gamma^0\}$, and

$$\lambda^{-1}(\gamma^0) \leqq \inf A(\rho_0) \leqq \inf A(\rho') + \inf A(\rho''),$$

where the first infimum is taken for all functions ρ_0 of the above form and the last two infima are taken for all admissible ρ' and $''\rho$. Consequently, $\lambda^{-1}(\gamma^0) \leqq \lambda^{-1}(\gamma') + \lambda^{-1}(\gamma'')$, and this contradicts the assumption that $\lambda(\gamma^0) = 0$.

1.7 The material of the present section is required in the third part of this paper. The proofs are simple applications of the comparison principle (Lemma 1) and Section 1.5 (a).

DEFINITION 3. ([2]) *Let* E_1 *and* E_2 *be closed disjoint subsets of the boundary of a region* Ω. *The extremal length of the family of crosscuts of*

Ω which have one endpoint on E_1 and the other on E_2 is called the extremal distance of E_1 and E_2 with respect to Ω, and it is denoted by $\lambda_\Omega(E_1, E_2)$.

In Section 1.5 (a), we saw that the extremal distance of the vertical sides of a rectangle of dimensions $a \times b$ is a/b; the extremal distance of the horizontal sides is b/a. We note that the product of these two extremal distances is 1.

We are concerned with the following configuration embedded in the unit disk K. Let E_1 be the right semicircular arc, $(+i, +1, -i)$, of the circumference of K, and let E_2 be the segment of the real axis from -1 to the point a $(-1 < a < +1)$. The upper semi-circular region is denoted by S.

LEMMA 3. *The extremal distance of $\bar{S}E_1$ and $\bar{S}E_2$ with respect to S is twice that of E_1 and E_2 with respect to $K - E_2$; in symbols: $\lambda_S(\bar{S}E_1, \bar{S}E_2) = 2\lambda_{K-E_2}(E_1, E_2)$.*

Proof. It is possible to map $K - E_2$ conformally and one-to-one onto a rectangle with horizontal and vertical sides of lengths u and v in such a way that E_1 corresponds to one and E_2 (traversed twice) to the other horizontal side. By conformal invariance, $\lambda_{K-E_2}(E_1, E_2) = v/u$. If the above rectangle is bisected by a vertical line, its right half will correspond to S under the inverse of the above map, and we have

$$\lambda_S(\bar{S}E_1, \bar{S}E_2) = v/(u/2) = 2\lambda_{K-E_2}(E_1, E_2).$$

LEMMA 4. *If E_3 is the left boundary arc of K, and E_4 is the segment of the real axis from the point a to $+1$, then*

$$\lambda_{K-E_4}(E_3, E_4) \cdot \lambda_{K-E_2}(E_1, E_2) = \tfrac{1}{4}.$$

Proof. This follows immediately, for by the preceding lemma we also have $\lambda_S(\bar{S}E_3, \bar{S}E_4) = 2\lambda_{K-E_4}(E_3, E_4)$, and in view of an earlier remark, $\lambda_S(\bar{S}E_3, SE_4) \cdot \lambda_S(\bar{S}E_1, SE_2) = 1$.

THEOREM 1. *The extremal length of the family $\{\gamma\}$ of crosscuts of K with endpoints on E_1 which separate the point a from E_3 is four times the extremal distance of E_1 and E_2 with respect to $K - E_2$.*

Proof. We first show

$$\lambda_K(\gamma) \leqq 2\lambda_S(\bar{S}E_1, \bar{S}E_2). \tag{1}$$

Let $\rho(z)$ be a function which is admissible for $\{\gamma\}$; we introduce the symmetrized function $\hat{\rho} = \rho + \bar{\rho}$, where $\bar{\rho}(z) = \rho(\bar{z})$, and $\bar{z}$ is the conjugate of z. Then $A_S(\hat{\rho}) \leqq 2A_K(\rho)$, since $A_S(\hat{\rho}) = \frac{1}{2}A_K(\hat{\rho})$ by symmetry, and an elementary estimate (Minkowski's inequality), together with the observation that $A_K(\rho) = A_K(\bar{\rho})$, shows $A_K(\hat{\rho}) \leqq 4A_K(\rho)$.

By $\{\delta\}$ we denote the family of crosscuts of S with endpoints on $\bar{S}E_1$ and $\bar{S}E_2$, respectively. If δ belongs to this family, it, together with $\bar{\delta}$, its reflection in the real axis, forms a crosscut of K which separates a from E_3 and has endpoints on E_1; in short, $\delta \cup \bar{\delta} = \gamma \in \{\gamma\}$. We have

$$L_{\{\gamma\}}(\rho) \leqq l_\rho(\gamma) = l_\rho(\delta \cup \bar{\delta}) = l_{\hat{\rho}}(\delta),$$

and hence, $L_{\{\gamma\}}(\rho) \leqq L_{\{\delta\}}(\hat{\rho})$, so that, since it is immediately verified that $\hat{\rho}$ is admissible for $\{\delta\}$ and S,

$$L_{\{\gamma\}}^2(\rho)/A_K(\rho) \leqq 2L_{\{\delta\}}^2(\hat{\rho})/A_S(\hat{\rho}) \leqq 2\lambda_S(\delta).$$

This relation holds for each ρ admissible for $\{\gamma\}$ and K, and thus we have formula (1).

Next, we have

$$(2) \qquad \lambda_K(\gamma) \geqq 4\lambda_{K-E_2}(E_1, E_2).$$

Namely, if $\{\delta'\}$ is the family of crosscuts of $K - E_2$ with endpoints on E_1 and E_2, respectively, we let ϵ be a positive number, and we consider a function $\rho(z)$, which is admissible for $\{\delta'\}$ and such that

$$L_{\{\delta'\}}^2(\rho)/A_{K-E_2}(\rho) > \lambda_{K-E_2}(\delta') - \epsilon/4.$$

Then we define $\rho_0(z)$ for $z \in K$ by placing

$$\rho_0(z) = \rho(z) \text{ if there is a } \delta' \text{ in } \{\delta'\} \text{ for which } z \in \delta',$$

and $\rho_0(z) = 0$ otherwise. Each $\gamma \in \{\gamma\}$ contains two arcs, δ'_1 and δ'_2, of the family $\{\delta'\}$. Consequently,

$$l_{\rho_0}(\gamma) \geqq l_{\rho_0}(\delta'_1) + l_{\rho_0}(\delta'_2) \geqq 2L_{\{\delta'\}}(\rho),$$

and hence, $L_{\{\gamma\}}(\rho_0) \geqq 2L_{\{\delta'\}}(\rho)$; also $A_K(\rho_0) \leqq A_{K-E_2}(\rho)$. From this it follows that

$$\lambda_K(\gamma) \geqq L_{\{\gamma\}}^2(\rho_0)/A_K(\rho_0) \geqq 4L_{\{\delta'\}}^2(\rho)/A_{K-E_2}(\rho) > 4\lambda_{K-E_2}(\delta') - \epsilon.$$

This holds for each positive ϵ, so that (2) is established. Formulas (1) and (2) together with Lemma 3, now yield the theorem.

II. Property P and Relation P^*. Prime Ends.

2.0 Summary. We consider sequences of points of a simply connected region on the Riemann sphere. A P-sequence is one for which the extremal length of a certain associated family of crosscuts is 0. We also introduce Q-sequences by a similar condition relating to a family of generalized crosscuts, and we show that $\{a_n\}$ is a Q-sequence if and only if it is also a P-sequence. Two sequences form a P^*-pair provided their join, the mixed sequence obtained from them, is a P-sequence. Then P^* is an equivalence relation defined on the P-sequences of the region. (It is the proof of the transitivity of the relation P^* which requires the consideration of Q-sequences.)

We shall see that the P^* equivalence classes of a circular disk are in one-to-one correspondence with the points of the circumference, and, in general, for a simply connected region, the P^* classes consist precisely of those P-sequences which converge to prime ends of the region in the sense of Carathédory. We may therefore identify these prime ends with our P^* equivalence clases. Since P-sequences and P^*-pairs are, by definition, conformally invariant concepts, we obtain an immediate proof of Carathédory's fundamental theorems.

2.1 Let Ω be a simply connected region, and let A and B be two sets contained in Ω. Then we say that the generalized crosscut τ of Ω separates A and B with respect to Ω, if $A \cup B \subset \{\Omega - (\tau)\}$, and if the set of components of $\Omega - (\tau)$ containing points of A is disjoint from the set of components containing points of B.

To formulate our principal definition, we consider a sequence $\{a_n\}$ of points of the region Ω, together with a closed subset E of Ω which has the property that a_n belongs to the set $\Omega - E$, except for at most a finite number of subscripts. With this configuration we associate two families of curves:

$\{\gamma\}$, the set of all crosscuts of Ω which separate E from almost all[3] a_n, and

$\{\tau\}$, the set of all generalized crosscuts of Ω each of which separates E from almost all a_n.

DEFINITION 4. *The sequence $\{a_n\}$ has Property P with respect to the set E, provided the associated family $\{\gamma\}$ has extremal length $\lambda(\gamma) = 0$.*

DEFINITION 4a. *The sequence $\{a_n\}$ has Property Q with respect to E, provided the associated family $\{\tau\}$ has extremal length $\lambda(\tau) = 0$.*

---

[3] As is customary, "almost all a_n" means "all a_n with at most a finite number of exceptions."

Remarks. 1. A sequence with Property P will be called a P-sequence, and similarly, one with Property Q, a Q-sequence.

2. The purpose of the family $\{\tau\}$ and of Property Q is to facilitate the proof of the transitivity of our relation P^* (see Definition 6 and Theorem 4 below).

3. Since $\{\gamma\} \subset \{\tau\}$, $\lambda(\gamma) = 0$ implies $\lambda(\tau) = 0$, by the comparison principle. We shall see in the sequel that it is true as well, that if $\lambda(\tau) = 0$ then $\lambda(\gamma) = 0$; hence the two properties, P and Q, are equivalent.

4. In Theorem 2, we shall see that Property P is independent of the set E; hence, it suffices to speak of P-sequences. When no explicit reference to a set E is made, we assume that there is a fixed closed subset E of Ω with respect to which a given sequence of points of the region either has or fails to have Property P.

LEMMA 5. *If $\{a_n\}$ is a P-sequence of Ω (with respect to a set E), then any subsequence is also a P-sequence.*

Proof. Clearly, almost all points of the subsequence belong to $\Omega - E$, and the family $\{\gamma'\}$, of crosscuts of Ω separating almost all points of the subsequence from E, contains the family $\{\gamma\}$. Hence, $\lambda(\gamma') \leqq \lambda(\gamma) = 0$, and the lemma is established.

LEMMA 6. *All accumulation points of the P-sequence $\{a_n\}$ lie on the boundary of the region Ω.*

Proof. Let $\alpha \in \Omega$ be an accumulation point of the sequence. Then $\alpha \notin E$, since otherwise $\{\gamma\}$ would be empty, and $\lambda(\gamma) = \infty$. Therefore, the open set $\Omega - E$ contains a closed disk Δ with center α such that $a_n \in \Delta$ for an infinite number of indices. If Π is a polynomial arc contained in Ω which connects α to a point β of E, then every crosscut γ of the family $\{\gamma\}$ intersects the continuum $\kappa = \Pi \cup \Delta$. Now, κ has positive spherical distance δ from the boundary. Let $\rho^*(z) = \psi(z, \infty)$, where $\psi(z, w)$ is the spherical distance. Then, for each $\gamma \in \{\gamma\}$, $l_{\rho^*}(\gamma) \geqq 2\delta$, and hence, $L_{\{\gamma\}}(\rho^*) \geqq 2\delta$. Since $0 < A(\rho^*) < \pi$, ρ^* is admissible, and we have

$$\lambda(\gamma) \geqq L^2(\rho^*)/A(\rho^*) \geqq (4/\pi)\delta^2 > 0.$$

This contradiction shows that α cannot be an interior point of the region.

2.2 THEOREM 2. *Let E' be any non-empty closed subset of Ω. Then, if $\{a_n\}$ has property P with respect to E, it also has property P with respect to the set E'.*

Proof. First of all, we note that almost all points a_n belong to $\Omega - E'$, for otherwise the sequence $\{a_n\}$ would have an accumulation point in E', contradicting Lemma 6. We denote by $\{\gamma'\}$ the family of crosscuts of Ω each of which separates E' from almost all a_n, and we show that if $\lambda(\gamma) = 0$ then $\lambda(\gamma') = 0$. Two special cases must be dealt with separately.

(a) If $E' \subset E$, every γ is also a γ'; the comparison principle (Corollary of Lemma 1) yields $\lambda(\gamma) \geqq \lambda(\gamma')$, so that $\lambda(\gamma') = 0$.

(b) Next we assume that E' is connected, and $E \subset E'$. The sets E' and $bd\,\Omega$ have a positive spherical distance δ, since they are closed and disjoint subsets of Σ. Again, we use the spherical metric, $\rho^*(z)\,|\,dz\,|$, and we consider the family of crosscuts $\{\gamma^0\} = \{\gamma\} - \{\gamma'\}$. If $\{\gamma^0\}$ is empty, $L_{\{\gamma^0\}}(\rho^*) = \infty$ by convention, and we have automatically that $\lambda(\gamma^0) > 0$. If $\{\gamma^0\}$ is not empty, it follows from the connectedness of E' that each γ^0 of this family intersects the set E'; hence, $l_{\rho^*}(\gamma^0) \geqq 2\delta$, and we may conclude as in the proof of the preceding lemma that $\lambda(\gamma^0) > 0$. Since $\{\gamma\} = \{\gamma'\} \cup \{\gamma^0\}$, Lemma 2, together with our assumption that $\lambda(\gamma) = 0$, implies that $\lambda(\gamma') = 0$.

(c) For the general case, where E and E' are arbitrary, we consider a closed and connected subset E^* of Ω which contains both E and E'. (A suitable set E^* can be constructed in view of Lemma 6.) By (b), the sequence $\{a_n\}$ is then a P-sequence with respect to E^*, and hence, by (a), it is also a P-sequence with respect to the set E'. This concludes the proof.

2.3 We now show that every Q-sequence is also a P-sequence.

LEMMA 7. *For every family $\{\tau\}$ of generalized crosscuts of Ω with $\lambda(\tau) = 0$, there is a point $\omega \in bd\,\Omega$ and a sequence $\{\tau_n\}$ of the family, such that the generalized crosscuts τ_n converge to the point ω, in the sense that the sequence $\{r_n\}$, defined by $r_n = \sup\{\psi(z,\omega)\,|\,z \in \tau_n\}$ converges to zero with $1/n$.*

Proof. The spherical metric, $\rho^*(z) = \psi(z,\infty)$, satisfies $0 < A(\rho^*) \leqq \pi$; hence, since $\lambda(\tau) = 0$, $L_{\{\tau\}}(\rho^*) = 0$. Consequently, there is a sequence $\{\tau_n\}$, contained in the family $\{\tau\}$, for which $l_{\rho^*}(\tau_n)$ decreases to 0. We choose a point b_n in each set (τ_n), and we show first that the sequence $\{b_n\}$ cannot have an accumulation point in the interior of the region Ω. For, if ω were such a point, let its spherical distance from the boundary be 3δ. Each τ_n meets the set of points of Ω whose spherical distance from the boundary is less than δ, and an infinite number of the τ_n also meet the spherical neighborhood of ω of radius δ. For these latter curves, we have then that

$l_{\rho^*}(\tau_n) \geqq \delta > 0$, and this contradicts the assumption that $l_{\rho^*}(\tau_n)$ decreases to 0.

We now choose an accumulation point ω of the sequence $\{b_n\}$. ω belongs to the boundary of the region Ω, by the preceding observation. Hence, there is a subsequence, which we again call $\{\tau_n\}$, with the property that the corresponding sequence of points $\{b_n\}$ converges to ω. Consequently, since $l_{\rho^*}(\tau_n)$ converges to zero, we have that $r_n \rightarrow 0$.

THEOREM 3. *Let E be a closed subset of the simply connected region Ω. Then the sequence of points $\{a_n\}$ ($a_n \in \Omega$) is a Q-sequence of Ω with respect to E if and only if it also is a P-sequence of Ω with respect to E.*

Proof. The necessity of the condition is obvious, in view of the Comparison Principle. For the sufficiency, we observe that by Lemma 7 there is a point ω on the boundary of Ω and a sequence $\{\tau_k\}$ contained in the family $\{\tau\}$ which converges to the point ω. Without loss of generality, we may assume that $\omega \neq \infty$. Then the sequence $\{r_k\}$, $r_k = \sup\{|z - \omega| \mid z \in \tau_k\}$ $(k = 1, 2, \cdots)$, converges to zero. Let C_k be the circle with center at ω and with radius r_k $(k = 0, 1, 2, \cdots)$, where r_0 is chosen so small that C_0 separates almost all the crosscuts τ_k from E. For each such k, every simple closed arc, which separates (in the plane) the circles C_0 and C_k, contains a crosscut (indeed a crosscut in the classical sense) which separates (with respect to Ω) E from almost all a_n and which thus belongs to the family $\{\gamma\}$. Consequently, denoting by $\{\delta_k\}$ the family of all such simple closed arcs, we have by Section 1.5 (b) and Lemma 1 that

$$\lambda(\gamma) \leqq \lambda(\delta_k) = 2\pi/\log(r_0/r_k).$$

The right side converges to zero as $k \rightarrow \infty$, and the result, $\lambda(\gamma) = 0$, follows.

2.4 DEFINITION 5. *If $\{a_n\}$ and $\{b_m\}$ are two sequences, their join is the sequence $\{c_k\}$, given by $c_{2k-1} = a_k$, and $c_{2k} = b_k$ $(k = 1, 2, \cdots)$.*

DEFINITION 6. *The sequences $\{a_n\}$ and $\{b_m\}$ of points of a simply connected region Ω form a P^*-pair if the join of these sequences is a P-sequence.*

Clearly, each sequence of a P^*-pair is itself a P-sequence, and by Theorem 3, a Q-sequence.

THEOREM 4. *The relation of being a P^*-pair is an equivalence relation on the P-sequences of a region Ω.*

Proof. The reflexivity and symmetry of P^* are obvious; it remains to show that this relation is also transitive. Let $\{a_i\}$, $\{b_j\}$, $\{c_k\}$ be three P-sequences of Ω, such that the first two and the last two form P^*-pairs. Let E be a closed subset of Ω containing at most a finite number of points of the three sequences. By $\{\tau_{ab}\}$, $\{\tau_{bc}\}$, and $\{\tau_{ac}\}$ we denote the families of generalized crosscuts of Ω which separate E from almost all points of the join's of the sequences indicated by the subscripts. In view of Theorem 3, we know from our hypothesis that

$$\lambda(\tau_{ab}) = \lambda(\tau_{bc}) = 0, \tag{1}$$

and we must show that $\lambda(\tau_{ac}) = 0$.

Now, let τ_1 and τ_2 belong to $\{\tau_{ab}\}$ and $\{\tau_{bc}\}$, respectively. The generalized curve, whose point set is $(\tau_1) \cup (\tau_2)$, separates E from almost all points of the join of $\{a_i\}$ and $\{c_k\}$. Hence, if $(\tau_1) \cup (\tau_2)$ is connected, it forms a member of $\{\tau_{ac}\}$. If, however, that set is not connected, then since each of (τ_1) and (τ_2) is connected, and both separate E from almost all points of $\{b_j\}$, one of (τ_1), (τ_2) must separate the other from E, and it, therefore, belongs to the family $\{\tau_{ac}\}$. Thus, the union of every pair τ_1, τ_2 contains a τ_{ac}. Let $\{\tau^*\}$ be the family of all τ_{ac} with the property that for each τ^* there is $\tau_1 \in \{\tau_{ab}\}$ and $\tau_2 \in \{\tau_{bc}\}$ and such that $\tau^* \subset \tau_1 \cup \tau_2$.

Then we have, for every non-negative function ρ on the region Ω and for every τ^*, that $l_\rho(\tau^*) \leqq l_\rho(\tau_1) + l_\rho(\tau_2)$, where τ_1 and τ_2 are the elements of $\{\tau_{ab}\}$ and $\{\tau_{bc}\}$, respectively, which correspond to τ^*. Hence,

$$L_{\{\tau^*\}}(\rho) \leqq l_\rho(\tau_1) + l_\rho(\tau_2),$$

and finally,

$$L_{\{\tau^*\}}(\rho) \leqq L_{\{\tau_{ab}\}}(\rho) + L_{\{\tau_{bc}\}}(\rho).$$

It is easily seen that ρ is admissible for $\{\tau^*\}$ if and only if it is admissible for both families $\{\tau_{ab}\}$ and $\{\tau_{bc}\}$. We may now restrict ourselves to functions ρ for which $A(\rho) < \infty$, and for these it follows from formula (1) that the right side of the preceding inequality vanishes. Hence, the same is true of the left side, and consequently,

$$\lambda(\tau^*) = \sup \{L^2_{\{\tau^*\}}(\rho)/A(\rho)\} = 0.$$

This, together with the fact that $\{\tau^*\} \subset \{\tau_{ac}\}$, concludes the proof.

2.5 In the case of the unit disk $K = \{z \mid |z| < 1\}$, there is a complete characterization of the P^* equivalence clases.

THEOREM 5. *A sequence $\{a_n\}$ of points of K is a P-sequence if and only if it converges to a point $\zeta = e^{i\theta}$ of the circumference of K.*

Proof.

(a) Let $\lim_{n\to\infty} a_n = \zeta$. We take the set consisting of the origin alone to be E, and set $r_j = |a_j - \zeta|$, and $C_j = \{z \mid |z-\zeta| = r_j\}$. The sequence $\{r_j\}$ converges to 0; without loss of generality we can, by restriction to a suitable subsequence of $\{a_n\}$, assume that C_1 separates C_n (for $n > 1$) from E. Then, if $\{\gamma\}$ is the family of crosscuts of K which separate E from almost all a_n, it follows as in the proof of Theorem 3 that $\lambda(\gamma) = 0$, and thus $\{a_n\}$ is a P-sequence of K.

(b) If $\zeta_1 = e^{i\theta_1}$ and $\zeta_2 = e^{i\theta_2}$ are distinct points of the circumference, let $\{a_m\}$ and $\{b_n\}$ be sequences converging to ζ_1 and ζ_2, respectively. Once more, let E be the set consisting of $z = 0$ only. Each member of the family $\{\gamma_{ab}\}$ of crosscuts of K which separate E from almost all points of the join of our two sequences has Euclidean length at least $|\zeta_1 - \zeta_2|$. Denoting by ρ_0 the function $\rho_0(z) \equiv 1$ for all z of K, we have $L_{\{\gamma_{ab}\}}(\rho_0) \geqq |\zeta_1 - \zeta_2|$, while $A(\rho_0) = \pi$; hence,

$$\lambda(\gamma_{ab}) \geqq \tfrac{1}{\pi} |\zeta_1 - \zeta_2|^2 > 0.$$

Consequently, a sequence of points of K with more than one accumulation point on the circumference cannot be a P-sequence.

From the theorem we immediately deduce the following consequence.

COROLLARY. *The P^* equivalence classes of a circular disk are in one-to-one correspondence with the points of its circumference.*

The correspondence in question is the one which assigns to each boundary point the family of all sequences converging to it.

We have remarked repeatedly on the fact that our definitions of P-sequence and P^*-equivalence are formulated in a conformally invariant manner. From this observation, we conclude that if Ω is mapped onto the unit disk K in accordance with the Riemann mapping theorem, then every P-sequence of Ω has an image which converges to a point of the circumference, and two P-sequences have images converging to the same point of the circumfeernce if and only if they form a P^*-pair. Conversely, every sequence of points of K which converges to a point ζ of the circumference is transformed by the inverse map into a P-sequence of the region Ω, and two sequences of K correspond to a P^*-pair if and only if they converge to the same point of the unit circumference.

2.6 We now demonstrate the equivalence of our theory with the classical one. First, we state Carathéodory's main definitions in a suitable form. Throughout this section, Ω will be a bounded simply connected region; that is the only situation considered by Carathéodory.

DEFINITION 7. *A sequence* $\{\gamma_n\}$ *of crosscuts*[4] *of* Ω *shall be called a chain of crosscuts of* Ω, *if*

(i) *for each* n, γ_{n+1} *separates* γ_n *and* γ_{n+2} (*in* Ω),

(ii) *there is a point* $\omega \in bd\,\Omega$ *such that each crosscut* γ_n *of the sequence is an arc of a circle* C_n *with center* ω *and radius* r_n, *and*

(iii) *the sequence* $\{r_n\}$ *decreases to* 0.

The point ω is called the *center* of the chain.

DEFINITION 8. *A sequence* $\{a_n\}$ *of points of* Ω *converges to the prime end determined by the chain of crosscuts* $\{\gamma_n\}$, *provided each crosscut of the chain separates almost all points* a_m *from the component of* $\Omega - \gamma_1$ *not containing* γ_2.

A prime end of Ω is an equivalence class of sequences converging to the same prime end.

A prime end may, of course, be defined by different chains, and these may have distinct centers. If ω can serve as the center of a chain of crosscuts defining a prime end, it is called a *principal point* of the prime end.

Carathéodory has proved the following result, which allows the conclusion that a sequence of points converges to a prime end under conditions on a sequence of crosscuts which do not require that it form a chain.

LEMMA 8. *Let* ω *be a point of the boundary of the bounded simply connected region* Ω, *and let* $\{\gamma_n\}$ *be a sequence of crosscuts which converge to* ω *in the sense that* $\sup_{z \in \gamma_n} |z - \omega| \to 0$. *Furthermore, let* $\{a_n\}$ *be a sequence of points of* Ω *such that each* γ_n *separates almost all* a_m *from a closed set* $E \subset \Omega$. *Then* $\{a_m\}$ *converges to a prime end of* Ω.

For the proof we refer to Carathéodory's paper [4; p. 338].

It is now an easy matter to prove the following theorem:

THEOREM 6. (a) *Each P-sequence* $\{a_n\}$ *of points of* Ω *converges to a prime end of* Ω, *and* (b) *each sequence which converges to a prime end is a P-sequence.*

---

[4] For Carathéodory, of course, "crosscut" meant crosscut in the classical sense (see Footnote 2). In view of an obvious modification of the argument of Lemma 7 and Theorem 3, it is not necessary for us to make this distinction here.

Proof. (a) It follows from Lemma 7 that the family of crosscuts $\{\gamma\}$ which separate E from almost all a_n contains a sequence of crosscuts converging to a point $\omega \in bd\,\Omega$. Therefore, Lemma 8 assures that the sequence $\{a_n\}$ converges to a prime end of Ω.

(b) The proof parallels that of Theorem 3. Let $\{\gamma_k\}$ be the chain of circular crosscuts defining the prime end, and let ω be its center. C_k and r_k have the meanings attached to these symbols in Definition 7 (ii). For E we take a closed subset of that component of $\Omega - (\gamma_1)$ which does not contain γ_2. Each simple closed curve, which separates (with respect to the plane) the circles C_1 and C_k, contains a crosscut of Ω separating γ_1 and γ_k (in Ω). This crosscut therefore separates almost all a_n from E. Hence, by Section 1. 5 (b) and Lemma 1, we have

$$\lambda(\gamma) \leqq 2\pi/\log(r_1/r_k),$$

and the right side converges to 0 as $k \to \infty$, since $\{r_k\}$ is a sequence which decreases to 0. Therefore, $\lambda(\gamma) = 0$, and the proof is complete.

2. 7 We now identify our P^*-equivalence classes with the prime ends of Carathéodory. Thus, we replace "$\{a_n\}$ is a P-sequence" by "$\{a_n\}$ converges to a prime end," and "$\{a_n\}$ and $\{b_m\}$ are a P^*-pair" by "$\{a_n\}$ and $\{b_m\}$ converges to the same prime end." Also, if Π is a prime end (i. e., a P^*-equivalence class) of the region Ω and $\{a_n\}$ a sequence of points of Ω, then "$\{a_n\} \in \Pi$" and "$\{a_n\}$ converges to Π" will be considered equivalent.

The following two theorems are Carathéodory's fundamental propositions.

THEOREM 7. *The prime ends of a (bounded) simply connected region are in one-one correspondence with the points of the unit circumference.*

Proof. In view of the conformal invariance of our definitions, this follows from Theorem 5 as we have already indicated in the remarks at the end of Section 2. 5.

THEOREM 8. *A sequence of points $\{a_n\}$ of a (bounded) simply connected region Ω either has an accumulation point in Ω, or it contains a subsequence which converges to a prime end of Ω.*

Proof. In the absence of an interior accumulation point, all accumulation point are on the boundary of Ω. We consider the image sequence $\{f(a_n)\}$, where $w = f(z)$ maps Ω conformally and one-one onto the unit disk K of the w-plane. All accumulation points of this image sequence lie on the circumference; we choose a sequence, which converges to a point of the circumference, and thus, to a prime end of K. The preceding theorem assures that the inverse image of this subsequence converges to a prime end of Ω.

DEFINITION 9. *The set of accumulation points of all P-sequences belonging to the P^*-class (the prime end)* Π *shall be called the point set of* Π; *we denote it by* (Π).

The point set (Π) of a prime end Π is a closed and connected subset of the boundary; it may reduce to a single point. The principal points of the prime end Π (see Section 2.6) belong to (Π); all other points of (Π) are called *subsidiary points* of Π. The following propositions are stated without proof [4]. The point set of each prime end contains at least one principal point; if it contains more than one, they form a closed connected set; also, there need not be any subsidiary points. In Part III, we shall give a sufficient condition that a P-sequence of points of Π has only principal points of its prime end for accumulation points.

For economy of language it is convenient to identify the prime ends of the unit disk with the points on the circumference to which all P-sequences of the equivalence class converge in view of Theorem 5. Thus, if ζ is a point of the circumference, we shall freely employ terminology like "the prime end ζ."

The correspondence of Theorem 7 is used to define the cyclic order of the prime ends of a simply connected region Ω. A segment of prime ends is a collection of prime ends corresponding to a segment of the circumference. The notion of cyclic order could also be introduced intrinsically, i.e. using only concepts and constructions relating to the region Ω. (See, for example, Kerékjártó's book ([5], p. 80), or the author's thesis.)

III. Central Convergence.

3.0 Summary. In this final section we study the structure of prime ends in more detail. Namely, at the end of Section 2.7, we distinguished between two types of points, principal and subsidiary, on the point set of a prime end. It is now our concern to place into a conformally invariant setting a theorem of Lindelöf which gives a sufficient condition that all accumulation points of a P-sequence be principal.

3.1 DEFINITION 10. *If all accumulation points of a P-sequence of points of* Ω *are principal points of the prime end to which the sequence converges, we call the sequence a principal P-sequence.*

Being a principal sequence in this sense is *not* a conformally invariant property. However, we give a sufficient condition that a P-sequence be principal; this condition, which adapts Lindelöf's theorem on approach in an angle, is a conformally invariant one. Indeed, with each point a_n of the P-sequence under consideration we associate an extremal length λ_n, and we formulate our theorem in terms of a certain boundedness condition on the sequence $\{\lambda_n\}$.

Suppose then that Π and Π^* are two prime ends of Ω which correspond, when Ω is mapped conformally and one-to-one onto K, to $+i$ and $-i$, respectively. Let α be the segment of prime ends corresponding, under the inverse of this map, to the (open) arc $(+i, -1, -i)$ of the circumference, and let α^* be the segment of prime ends corresponding to the open arc $(-i, +1, +i)$. Again indicating point sets of prime ends by parentheses, we have

$$bd\,\Omega = (\Pi) \cup (\alpha) \cup (\Pi^*) \cup (\alpha^*).$$

Of course, the preceding is not, in general, a union of disjoint sets.

We shall say that a crosscut of the region Ω terminates on the segment α if every P-sequence of points of Ω which lies on the crosscut belongs to a prime end of α.

With a point $a \in \Omega$ and the pair of prime ends Π and Π^* of Ω we associate two families of crosscuts of Ω, $\{\gamma\}$ and $\{\gamma^*\}$. Namely, each $\gamma \in \{\gamma\}$ shall separate the point a from α^* and terminate on α; the family $\{\gamma^*\}$ is defined dually. From Theorem 1, we have that

$$\lambda(\gamma) \cdot \lambda(\gamma^*) = 4. \tag{1}$$

This formula also follows from an explicit computation of $\lambda(\gamma)$; in fact,

$$\lambda(\gamma) = 4\nu(\cos \tfrac{1}{2}\pi\omega_\alpha(a)), \tag{2}$$

where $\omega_\alpha(a)$ is the harmonic measure with respect to Ω of the segment α at a, $\nu(r) = \frac{1}{2}K^*(r)/K(r)$,

$$K(r) = \int_0^1 [(1-x^2)(1-r^2x^2)]^{-\frac{1}{2}}\,dx,$$

and $K^*(r) = K((1-r^2)^{\frac{1}{2}})$.

3.2 DEFINITION 11. *If $\{a_j\}$ is a P-sequence belonging to the prime end Π, then it is a central P-sequence, provided the associated sequence of positive numbers, $\{\lambda(\gamma_j) + 1/\lambda(\gamma_j)\}$ is bounded.*

It is a consequence of formula (2), above, that this definition is independent of the auxiliary prime end Π^*.

In view of formula (1) of Section 3.1, $\{a_j\}$ is a central P-sequence if and only if neither of the sequences $\{\lambda(\gamma_j)\}$ nor $\{\lambda(\gamma^*_j)\}$ has a subsequence which converges to either 0 or ∞.

The theorem of Lindelöf [6; p. 28] reads, in terms of central convergence, as follows.

THEOREM 9. *If* $\{a_j\}$ *is a central P-sequence of points of* Ω, *then* $\{a_j\}$ *is a principal P-sequence.*

Proof. We suppose that an accumulation point of the P-sequence $\{a_j\}$, say ω, is a subsidiary point of the prime end Π to which the sequences converges; we show that no subsequence, which converges to ω, can be a central P-sequence. It follows that the original sequence was not central.

Let the sequence $\{a_j\}$ converge to the subsidiary point ω; for convenience we assume $\omega \neq \infty$. We choose a prime end Π^* of Ω distinct from Π and a P-sequence $\{b_k\}$ which belongs to Π^*. Now let C be a circle with center at the point ω and radius r. Let the positive number r be so small that (a) almost all a_j lie inside C, (b) almost all b_k lie outside C, and (c) none of the arcs of $\Omega \cap (C)$ separates the set E (employed in the definition of the prime ends Π and Π^*) from almost all a_j. This choice of r is always possible, since $a_j \rightarrow \omega$, $\Pi^* \neq \Pi$, and ω is a subsidiary point of Π.

If σ_j is a crosscut of Ω which lies on C and which separates a_j from E, it has both its endpoints on the segment α, or it has both endpoints on α^*. The collection $\{\sigma_j\}$ is not finite, because of (a) and (c). Therefore, there must actually be an infinite number of distinct crosscuts σ_j whose endpoints are either both on α or on α^*.

Without loss of generality, we now assume that an infinite number of the σ_j have endpoints on α^*; we restrict ourselves to those values of the subscript j for which this condition holds. By Ω_j we denote the component of $\Omega - (\sigma_j)$ which contains a_j. Then every prime end of Ω_j that does not belong to σ_j is also a prime end of the region Ω, and it belongs to the segment α^*. Consequently, every crosscut γ of the family $\{\gamma_j\}$ must contain a crosscut of Ω_j both of whose endpoints lie on σ_j, and which intersects the circle C_j with center at ω and radius $r_j = |a_j - \omega|$.

Hence, every crosscut of $\{\gamma_j\}$ contains a crosscut of the family connecting C and C_j. From Lemma 1 and Section 1.5 (b), we now deduce that

$$\lambda(\gamma_j) \geqq \tfrac{1}{2\pi} \log (r/r_j),$$

so that $\lambda(\gamma_j) \rightarrow \infty$, since $r_j \rightarrow 0$. This shows that $\{a_j\}$ is not a central P-sequence. The proof is complete.

YALE UNIVERSITY.

REFERENCES.

[1] L. V. Ahlfors, *Conformal Mapping.* Lecture notes (transcribed by R. Osserman), Oklahoma A. and M. College, 1951.

[2] L. V. Ahlfors and A. Beurling, "Conformal Invariants," in *Construction and Applications of Conformal Maps (Proceedings of a Symposium)*, Washington, D. C., National Bureau of Standards, Applied Mathematics Series, No. 18, 1952.

[3] L. V. Ahlfors and A. Beurling, "Conformal invariants and function-theoretic null-sets," *Acta Mathematica,* vol. 83 (1950), pp. 101-129.

[4] C. Carathéodory, "Über die Begrenzung einfach zusammenhangender Gebiete," *Mathematische Annalen,* vol. 73 (1913), pp. 323-370.

[5] B. v. Keréjártó, *Vorlesungen über Topologie,* vol. 1, Berlin, J. Springer, 1923.

[6] E. Lindelöf, "Sur un principe général de l'analyse et ses applications à la théorie de la représentation conforme," *Acta Societatis Scientiarum Fennicae,* vol. 46 (1915), No. 4, pp. 1-35.

[7] S. Mazurkiewicz, "Über die Definition der Primenden," *Fundamenta Mathematicae,* vol. 26 (1936), pp. 272-279.

[8] H. Renggli, "Zur konformen Abbildung auf Normalgebiete," *Commentarii Mathematici Helvetici,* vol. 31 (1956), pp. 5-40.

[9] H. D. Ursell and L. C. Young, "Remarks on the theory of prime ends," *Memoirs of the American Mathematical Society,* No. 3 (1951).

ALGEBRAIC GROUPS AND THE GALOIS THEORY OF DIFFERENTIAL FIELDS.*

By Ellis Kolchin[1] and Serge Lang.

The purpose of this note is to draw together morely closely the Galois theory of differential fields and the theory of algebraic groups and homogeneous spaces.

Given a strongly normal extension of a differential field of characteristic 0, it is known (see [2] or Matsumura [3]) that the Galois group is isomorphic to the group of points of an algebraic group which are rational over the field of constants. We show below that the extension itself has a model which is a principal homogeneous space for the algebraic group, such that the operation of the elements of the Galois group on the extension is induced by the operation of the corresponding elements of the algebraic group on the space. The Galois theory can then be deduced from known facts concerning principal homogeneous spaces (Rosenlicht [4]). This provides an analysis of the Galois theory into two parts, one depending on the foundations of differential algebra and the other on the foundations of the theory of algebraic groups.

There remains almost untouched a converse problem which, for the sake of simplicity, we state for connected algebraic groups, or as we shall also say, group varieties. Given a differential field F of characteristic 0 with algebraically closed field of constants C, a group variety G defined over C, and a principal homogeneous space V for G defined over F, to determine all extensions of the differential field structure on F to the function field $F(V)$ which makes $F(V)$ a strongly normal extension of F with automorphism group induced by the group G_C of points of G rational over C. Put another way, the problem is to describe all possible ways of extending the derivation operators of F to derivation operators on $F(V)$ which are invariant relative to G_C, which commute with each other, and which have precisely C as field of constants. We observe here merely that the first condition alone

---

* Received August 3, 1957.

[1] The work of this author was assisted by a grant from the National Science Foundation.

presents no difficulty, i.e. that it is easily shown that the derivations of F can be extended to invariant derivations of $F(V)$.

1. Algebraic groups.

We recall here briefly the notions of algebraic group and principal homogeneous space. For the general theory, see Weil [5] and [6], and Rosenlicht [4].

An *algebraic set* V is a finite union of varieties, $V = \bigcup V_i$, which for the purposes of this paper we shall always assume disjoints; the V_i are the components of V. Let V, W be two algebraic sets. A rational map $f: V \to W$ is an algebraic set, having one component f_i for each component V_i of V such that f_i is a rational map in the usual sense of V_i into a component of W. We say that f is defined at a point $u \in U_i$ if f_i is defined at that point, and we write $f(u) = f_i(u)$.

An *algebraic group* is an algebraic set G together with an everywhere defined rational map of $G \times G$ into G, relative to which G is a group, having the further property that the inverse mapping $x \to x^{-1}$ is an everywhere defined rational map of G into G.

If G is an algebraic group, a *transformation space* for G is an algebraic set V together with an everywhere defined rational map of $V \times G$ into V (the operation of G on V) which, if we denote the image of (v, x) by vx, satisfies the conditions

$$v(xy) = (vx)y \text{ and } ve = v$$

for all $v \in V$, $x \in G$, $y \in G$ (e denoting the unity element of G.) A transformation space is a *homogeneous space* if, given any $v, w \in V$, there exists an $x \in G$ such that $vx = w$. The homogeneous space is *principal* if this point x is determined uniquely and rationally. By the latter we mean that there exists an everywhere defined rational map $\lambda: V \times V \to G$ such that $x = \lambda(v, w)$. If V is a principal homogeneous space for G then the number of components of V equals that of G and each component of V is a principal homogeneous space for the component G_0 of G containing e, G_0 being a normal subgroup of G the cosets of which are precisely the components of G.

We shall say that the algebraic group G is defined over a field k if all the components of G, of its group law, and of its inverse mappings are defined over k. Similarly, we shall say that the principal homogeneous space V for G is defined over k if G is defined over k, and if all the components of V, of the operation of G on V, and of λ are also defined over k. Although this notion of field of definition may present some drawbacks, it is adequate for our present purpose.

2. Differential-algebraic preliminaries. Let F be a differential field of characteristic 0. Denote the field of constants of F by C. We work in a fixed universal extension F^* of F in the sense of [1], and denote the field of constants of F^* by C^*. The facts stated in the following propositions were proved in [1].

Proposition 1. *The fields F and C^* are linearly disjoint over C.*

By an extension of F, we shall always mean a differential field extension contained in the universal domain. Similarly, an isomorphism will always mean a differential field isomorphism. When we wish to consider only the field structure, we shall say field extension, and field isomorphism.

Let E be an extension of F, and suppose that as a field extension E is finitely generated. Let F_0 be the algebraic closure of F in E. We recall if σ and σ' are isomorphisms of E, σ' is called a *specialization* of σ if the family $(\sigma'\alpha)_{\alpha\in E}$ is a specialization of $(\sigma\alpha)_{\alpha\in E}$ over E in the usual sense of algebraic geometry. The specialization is called *generic* if also σ is a specialization of σ'. An isomorphism of E over F is called *isolated* if it is not a nongeneric specialization of any isomorphism of E over F.

Proposition 2. (a) *There exists a finite set of isolated isomorphisms of E over F such that every isomorphism of E over F is a specialization of precisely one of these.*

(b) *An isomorphism σ of E over F is isolated if and only if the transcendence degree of the compositum $E\cdot\sigma E$ over E equals that of E over F.*

(c) *An alement of E invariant under an isolated isomorphism of E over F belongs to F_0.*

(d) *If σ is isolated then σ' is a specialization of σ if and only if their restriction to F_0 coincide. Every isomorphism of F_0 over F is the restriction to F_0 of an isolated isomorphism of E over F.*

Suppose further that E has the same field of constants C as F has, and that C is algebraically closed. We recall that an isomorphism σ of E is called *strong* if $\sigma E \subset E\cdot C^*$ and $E \subset \sigma E\cdot C^*$. Letting $C(\sigma)$ denote the field of constants of $E\cdot\sigma E$, we can see with the help of Proposition 1 that σ is strong if and only if

$$E\cdot C(\sigma) = E\cdot\sigma E = \sigma E\cdot C(\sigma).$$

Every automorphism of E is obviously a strong isomorphism of E.

PROPOSITION 3. (a) *Every strong isomorphism of E over F has a specialization which is an automorphism of E.*

(b) *An isomorphism of E over F is strong if and only if it is the restriction to E of an automorphism of $E \cdot C^*$ over $F \cdot C^*$.*

As the automorphism mentioned in (b) is evidently unique, we may identify the strong isomorphism with it. The set of strong isomorphisms of E over F is then identified with the group of automorphisms of $E \cdot C^*$ over $F \cdot C^*$. We denote this group by $\mathfrak{G}$.

Let $\sigma, \tau \in \mathfrak{G}$. As $C(\sigma^{-1})$ is the field of constants of $E \cdot \sigma^{-1}E$, $\sigma C(\sigma^{-1}) = C(\sigma^{-1})$ must be the field of constants of $\sigma(E \cdot \sigma^{-1}E) = E \cdot \sigma E$. Thus

$$C(\sigma^{-1}) = C(\sigma).$$

Writing $C(\sigma, \tau)$ to denote the compositum $C(\sigma) \cdot C(\tau)$, we see that

$$E \cdot C(\sigma, \sigma\tau) = E \cdot C(\sigma) \cdot C(\sigma\tau) = E \cdot \sigma E \cdot \sigma\tau E = E \cdot \sigma(E \cdot \tau E) = E \cdot \sigma(E \cdot C(\tau))$$
$$= E \cdot \sigma E \cdot C(\tau) = E \cdot C(\sigma) \cdot C(\tau) = E \cdot C(\sigma, \tau).$$

It follows with the help of Proposition 1 (applied to E instead of F) that $C(\sigma, \tau) = C(\sigma, \sigma\tau)$. Therefore $C(\tau^{-1}, \sigma^{-1}) = C(\tau^{-1}, \tau^{-1}\sigma^{-1}) = C(\tau, \sigma\tau)$. Thus

$$C(\sigma, \sigma\tau) = C(\sigma, \tau) = C(\sigma\tau, \tau). \tag{1}$$

We observe also, using Propositions 2(b) and Proposition 1, that $\sigma \in \mathfrak{G}$ is isolated if and only if the transcendence degree of $C(\sigma)$ over C equals that of E over F.

We suppose, finally, that the extension E of F is *strongly normal,* that is, that in addition to all the hypotheses made above, every isomorphism of E over F is strong. $\mathfrak{G}$ is then called the *Galois group* of E over F.

3. The theorem and its proof. We temporarily impose the restriction that $F = F_0$. Then by Proposition 2(a) and (d), all isolated elements of $\mathfrak{G}$ are generic specializations of each other.

Let $\sigma_0 \in \mathfrak{G}$ be isolated, and let W be any model of the field $C(\sigma_0)$ over C. This means that W is a variety defined over C and there exists a generic point x of W over C such that $C(\sigma_0) = C(x)$. If σ is any isolated element of $\mathfrak{G}$ then σ is a generic specialization of σ_0 so that there exists an isomorphism $E \cdot \sigma_0 E \approx E \cdot \sigma E$ over E mapping $\sigma_0\alpha$ onto $\sigma\alpha$ $(\alpha \in E)$. This isomorphism maps $C(\sigma_0)$ onto $C(\sigma)$ and therefore maps x onto a generic point of W over C, which we call x_σ (so that in particular $x_{\sigma_0} = x$) and which has the property that $C(\sigma) = C(x_\sigma)$. Because $E \cdot \sigma_0 E = E \cdot C(\sigma_0)$ the isomorphism $E\cdot\sigma_0 E \approx E\cdot\sigma E$ over E is determined by its restriction to $C(\sigma_0)$, so that σ is determined by x_σ.

Furthermore if y is any point of W which is rational over C^* and generic over C, there exists a unique field isomorphism $C(x)\approx C(y)$ over C mapping x onto y, and because E and C^* are linearly disjoint over C this field isomorphism can be extended to a field isomorphism ϕ over E of $E\cdot C(x) = E\cdot C(\sigma_0) = E\cdot\sigma_0 E$ onto $E\cdot C(y)$. As ϕ maps $C(\sigma)$ into $C(y)$, ϕ commutes on $C(\sigma)$ with the derivation operators of the differential field structure, and as ϕ is the identity on E, ϕ commutes on E with these derivation operators, so that ϕ commutes on $E\cdot C(\sigma)$ with these operators. In other words, ϕ is a differential field isomorphism. Letting $\tau=\phi\sigma_0$, we see that $y=x_\tau$. We have thus proved that $\sigma\rightarrow x_\sigma$ is a bijective mapping of the set of isolated elements of G onto the set of points of W which are rational over C^* and generic over C.

Let $\sigma,\tau\in\mathfrak{G}$. If in addition to being isolated, σ and τ are independent, in the sense that $C(\sigma)$ and $C(\tau)$ are linearly disjoint over C, then (1) shows that $\sigma\tau$ is isolated. Furthermore, by Proposition 1, $E\cdot\sigma E = E\cdot C(\sigma)$ and $E\cdot\tau E = E\cdot C(\tau)$ are linearly disjoint over E. If σ' and τ' are also independent isolated elements of $\mathfrak{G}$, then the isomorphism $E\cdot\sigma E\approx E\cdot\sigma' E$ over E mapping $(\sigma\alpha)_{\alpha\in E}$ onto $(\sigma'\alpha)_{\alpha\in E}$ and the analogous isomorphism $E\cdot\tau E \approx E\cdot\tau' E$ have a unique common extension.

$$E\cdot\sigma E\cdot\tau E\approx E\cdot\sigma' E\cdot\tau' E. \tag{2}$$

For any element $\alpha\in E$, $\tau\alpha$ can be expressed in the form $\tau\alpha=f(x_\tau)$, where f is a rational function on W defined over E. Hence we have $\tau'\alpha=f(x_{\tau'})$, $\sigma\tau\alpha=f^\sigma(x_\tau)$, and $\sigma'\tau'\alpha=f^{\sigma'}(x_{\tau'})$. From this it is clear that the isomorphism (2) maps $(\sigma\tau\alpha)_{\alpha\in E}$ onto $(\sigma'\tau'\alpha)_{\alpha\in E}$ and therefore maps $x_{\sigma\tau}$ onto $x_{\sigma'\tau'}$. Thus $(x_{\sigma'}, x_{\tau'}, x_{\sigma'\tau'})$ is a specialization of $(x_\sigma, x_\tau, x_{\sigma\tau})$ over C (and even over E).

It follows that we may define a law of composition on W by the formula $x_\sigma x_\tau = x_{\sigma\tau}$, this law of composition being defined over C. From (1) we have $C(x_\sigma, x_\sigma x_\tau) = C(x_\sigma, x_\tau) = C(x_\sigma x_\tau, x_\tau)$. Furthermore, if ω is an isolated element of $\mathfrak{G}$ such that ω,σ,τ are independent, i.e. such that $x_\omega, x_\sigma, x_\tau$ are independent generic points of W, then it is clear that $x_\omega(x_\sigma x_\tau) = (x_\omega x_\sigma)x_\tau$. Thus we have a normal law of composition on W, so that by the fundamental theorem of Wiel [5], W is birationally equivalent over C to a group variety defined over C. Thus we may suppose that W is itself a group variety, and we henceforth denote it by G.

Since we have assumed that $F=F_0$, E is a regular extension of F.

Therefore there exists a model V for E over F, i. e. a variety V defined over F such that E may be written $E = F(v)$ where v is a generic point of V over F. Letting σ be an isolated element of $\mathfrak{G}$, so that x_σ is a point of G which is rational over C^* and generic over C (and therefore over E), we define a rational map of $V \times G$ into V by the formula

$$(v, x_\sigma) \to vx_\sigma = \sigma v.$$

It follows from the above considerations that this rational map, which is defined over F, does not depend on which isolated element σ is used. It is also easy to see from what precedes that if σ and τ are independent isolated elements of $\mathfrak{G}$, then

$$F(vx_\sigma, x_\sigma) = F(v, x_\sigma) = F(v, vx_\sigma)$$

and

$$v(x_\sigma x_\tau) = (vx_\sigma)x_\tau.$$

It follows from another result of Weil ([6] Prop. 3) that V is birationally equivalent over F to a principal homogeneous space for G defined over F, and therefore we may assume that V itself is such a space. This principal homogeneous space is, moreover, uniquely determined up to an everywhere defined birational correspondence compatible with the operation of G.

This being the case, we see that every point $a \in G$ (generic or not) such that v is generic on V over $F(a)$ induces a field isomorphism σ_a of $E = F(v)$ over F mapping v onto va. If a is any point of the group G_{C^*} of points of G rational over C^*, then v is automatically generic on V over $F(a)$, because E and C^* are linearly disjoint over C, and hence E and $F \cdot C^*$ are linearly disjoint over F. In this case, σ_a is an isomorphism of the differential field structure. Indeed, for elements of G_{C^*} which are generic over C this has been proved above, and for an arbitrary $a \in G_{C^*}$, there exists an element $x \in G_{C^*}$ such that x^{-1} and xa are generic over C, and $\sigma_a = \sigma_{x^{-1}}\sigma_{xa}$.

The mapping $a \to \sigma_a$ $(a \in G_{C^*})$ is obviously an isomorphism of G_{C^*} into $\mathfrak{G}$. It is actually onto $\mathfrak{G}$, for given any $\tau \in \mathfrak{G}$ we can select an isolated $\tau' \in \mathfrak{G}$ so that τ and τ' are independent. Then $\tau\tau'$ and τ'^{-1} are isolated and $\tau = (\tau\tau')\tau'^{-1}$.

We have now proved our main result in the special case that $F = F_0$. We shall indicate below how to extend it to the general case, and we state here the general theorem which for the case $F = F_0$ summarizes the above discussion.

THEOREM. *Let F be a differential field of characteristic* 0 *with algebraically closed field of constants C, and let E be a strongly normal extension* *of F, all lying in a universal extension F^* with field of constants C^*. Let $\mathfrak{G}$ be the Galois group of E over F. Then there exists an algebraic group G defined over C, and a principal homogeneous spave V for G, defined over the algebraic closure F_0 of F in E, having the following properties.*

(a) *V is a model of E over F, that is, any component of V has a point v generic over F_0 such that $E = F_0(v)$, and these components are all conjugates to each other over F.*

(b) *For each $\sigma \in \mathfrak{G}$ there exists a unique point $x_\sigma \in G_{C^*}$ (the group of points of G which are rational over C^*) such that $\sigma v = v x_\sigma$, and the mapping $\sigma \rightarrow x_\sigma$ $(\sigma \in \mathfrak{G})$ is a group isomorphism of $\mathfrak{G}$ onto G_{C^*}.*

(c) *This isomorphism is rational in the sense that $C(\sigma) = C(x_\sigma)$ and that σ' is a specialization of σ if and only if $x_{\sigma'}$ is a specialization of x_σ over C.*

In order to extend the result proved for $F = F_0$ to the general case, we apply the proved result to the extension E of F_0. We thus obtain a connected algebraic group G_0 defined over C and a principal homogeneous space V_0 defined over F_0 such that V_0 has a point v generic over F_0 with $E = F_0(v)$, and the Galois group $\mathfrak{G}_0$ of E over F_0 is isomorphic with G_{0C^*} in the manner described in the statement of the theorem. Every $\sigma \in \mathfrak{G}$ maps F_0 onto the set of elements of σE which are algebraic over F, so that if σ is an automorphism of E then $\sigma F_0 = F_0$. Since by Proposition 3, σ always has a specialization which is an automorphism of E, which by Proposition 2(d) coincides with σ on F_0, we see that $\sigma F = F_0$ for every $\sigma \in \mathfrak{G}$. It now follows by Proposition 2(d) and (a) that the mapping

$$\sigma \rightarrow \text{restriction of } \sigma \text{ to } F_0$$

is a homomorphism of $\mathfrak{G}$ with kernel $\mathfrak{G}_0$ onto a finite group of automorphism of F_0 with fixed field F. If σ_i $(i = 1, \cdots, r)$ are the elements of the finite set of itsolated isomorphisms mentioned in Proposition 2(a) (with say $\sigma_0 \in \mathfrak{G}_0$) and if $\mathfrak{G}_i$ is the set of specializations of σ_i, then the $\mathfrak{G}_i$ are cosets of $\mathfrak{G}_0$ in $\mathfrak{G}$.

Using the fact (Proposition 3(a)) that each $\mathfrak{G}_i$ contains an element σ_i' which is an automorphism of E, we follow [2] to extend the isomorphism $\mathfrak{G}_0 \approx G_0$ to an isomorphism $\mathfrak{G} \approx G$ (rational in the sense of (c)), where G is an algebraic group of which the component of the unity element is G_0. The varieties $V_i = V_0^{\sigma_i'}$ determined by the restrictions of the σ_i' to F_0 are precisely the conjugates of V_0 over F, and for each i the point $v_i = \sigma_i' v_0$ is a generic point of V_i over F_0. We now define the operation of G on the algebraic set $V = \bigcup V_i$ in the obvious manner, namely by setting $v_i x_{\sigma_j} = \sigma_j v_i$ for all i and j. We leave to the reader the verification that this makes V into a principal homogeneous space for G with the stated properties.

Columbia University.

REFERENCES.

[1] E. R. Kolchin, " Galois theory of differential fields," *American Journal of Mathematics*, vol. 75 (1953), pp. 753-824.

[2] ———, " On the Galois theory of differential fields," *American Journal of Mathematics*, vol. 77 (1955), pp. 868-894.

[3] H. Matsumura, "Automorphism-groups of differential fields and group varieties," *Memoirs of the College of Science, University of Kyoto, Series A*, vol. 28 (1954), pp. 283-292.

[4] M. Rosenlicht, " Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp. 401-443.

[5] A. Weil, " On algebraic groups of transformation," *American Journal of Mathematics*, vol. 77 (1955), pp. 355-391.

[6] ———, " On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955), pp. 493-512.

STRATIFICATIONS OF CAUCHY'S "STABLE" TRANSCENDENTS AND OF MITTAG-LEFFLER'S ENTIRE FUNCTIONS.*

By AUREL WINTNER.

---

1. Let $\alpha > 0$ and, if x is real and $0 \leqq q < 1$, put

$$\theta_\alpha(x, q) = 1 + 2 \sum_{n=1}^{\infty} q^{n^\alpha} \cos nx.$$

What will be proved below, when combined with a known procedure based on Poisson's summation formula (cf. [13]), leads to the following result: Whenever $\beta > \alpha$, there exists on the interval $0 \leqq r < 1$ a *monotone* bounded function $\lambda(r) = \lambda_{\alpha\beta}{}^{q}(r)$ in such a way that

$$\theta_\alpha(x, q) = \int_0^{1-0} \theta_\beta(x, r)\, d\lambda_{\alpha\beta}{}^{q}(r) \qquad (d\lambda = d_r\lambda \geqq 0).$$

Since $\theta_2(x, q)$ is an elliptic theta-function which, in view of its Eulerian factorization, is positive throughout, there follows, as a corollary ($\beta = 2$), the known fact that $\theta_\alpha(x, q) > 0$ holds for every real x and for every positive $q < 1$ whenever $\alpha \leqq 2$. The integral formula becomes curious also under the stricter assumption $\alpha < 1$, since $\theta_\beta(x, q)$ is Poisson's explicit function $(1 - 2q \cos x + q^2)^{-1}$ if $\beta = 1$. But the point in the general "stratification" rule of $\theta_\alpha(x, q)$ is that arbitrarily large values of β, and any positive α which is less than β, are allowed for every positive $q < 1$. Of particular interest are the cases $\beta = 4, 6, \cdots$, occurring in the Hardy-Littlewood treatment of Waring's problem.

2. It was shown by Cauchy ([2], pp. 99-101) that the densities of probability $F(x)$, $-\infty < x < \infty$, of what today are called symmetric stable distributions must be the Fourier transforms $F(x) = F_\alpha(x)$ of the functions $\exp(-|t|^\alpha)$, where $\alpha > 0$; so that, if $x \geqq 0$ and $t \geqq 0$ without loss of generality, then

$$F_\alpha(x) = \tfrac{1}{\pi} \int_0^\infty \exp(-t^\alpha) \cos xt \, dt \tag{1}$$

---

* Received October 8, 1957.

(the Fourier transform of (1) is absolutely convergent, since $F_\alpha(x) = O(x^{-a})$, where $a = 1 + \alpha > 0$, and even $x^a F(x) \rightarrow c$, where $c = c(a)$, holds as $x \rightarrow \infty$, with $c(a) = 0$ if and only if $a = 2, 4, 6, \cdots$; cf. [11], p. 187). Cauchy's result on (1) the "stability" of (1) was rediscovered by Edgeworth [4] (Pizzetti's analysis of the questions involved mentions only Edgeworth; cf. [9], p. 114).

Cauchy and his immediate successors tacitly assumed that every function (1) actually is a density function, which would mean that $F_\alpha(x) \geqq 0$ holds for all x whenever $\alpha > 0$ (and Cauchy found for $\alpha > 2$ the curious "paradox," forgotten in the meantime, which is quoted by Czuber [3], p. 184). But it was observed by F. Bernstein [1] that this cannot be the case if $n = 4$ (and his method, adapted from Hardy's proof for the existence of an infinity of odd zeros on the critical line of the Riemann zeta-function, applies to $n = 6, 8, \cdots$ also).

The final result is due to P. Lévy (cf., e.g., [6], chap. VI of the second part, or [8], chap. V), who proved that $F_\alpha(x) \geqq 0$ holds for every x if and only if $\alpha \leqq 2$. But while the necessity of $\alpha \leqq 2$ can be proved easily, most proofs for the sufficiency of $\alpha \leqq 2$ are variants of one and the same existence consideration.

In what follows, the existence statement will be modified so as to contain a result which holds for *every* $\alpha > 0$ (i.e., not only for $\alpha \leqq 2$) and to contain, nevertheless, Lévy's result ($F_\alpha \geqq 0$) if $\alpha \leqq 2$ (even though the latter result cannot be true if $\alpha > 2$). In fact, it turns out that, *whenever* $0 < \alpha < \beta < \infty$, *there exists on the half-line* $0 \leqq u < \infty$ *a monotone function* $\phi(u) = \phi_{\alpha\beta}(u)$ *satisfying* $\phi(0) = 0$, $\phi(\infty) = 1$ *and*

$$(2) \qquad F_\alpha(x) = \int_0^\infty F_\beta(xu)\, d\phi_{\alpha\beta}(u) \qquad (d\phi_{\alpha\beta}(u) \geqq 0)$$

($0 \leqq x < \infty$). Since (1) reduces to $C \exp(-\tfrac{1}{2}x^2) > 0$ if $\alpha = 2$, the case $\beta = 2$ of (2) proves that not only $F_\alpha(x) \geqq 0$ but even

$$(3) \qquad F_\alpha(x) > 0 \text{ for all } x \text{ if } \alpha \leqq 2.$$

But the point is that (2) holds for every β (even for $\beta > 2$; e.g., for $\beta = 4, 6, \cdots$) whenever $\alpha < \beta$ (concerning the case of $F_\beta(x)$ when β is an even integer exceeding 2, cf. Pólya's note [11] and his asymptotic formula which I quoted on p. 834 of vol. 78 (1956) of this Journal).

It will also follow that, whenever $0 < \alpha < \beta < \infty$, the distribution $\phi_{\alpha\beta}(u)$ occurring in (2) is absolutely continuous on the closed half-line $[0, \infty)$ and regular (in the sense of analyticity) at every point u of the open half-line $(0,\infty)$.

3. For the point of departure in the proof of the first italicized theorem, it is possible to choose (among various, substantially equivalent choices; cf. e.g., the second paragraph of § 5 below) the existence of those "stable distributions" which may be called *unilateral*. These distributions, which in contrast to the *symmetric* stable distributions (which exist for $\alpha \leqq 2$; cf. § 2), exist only for $\alpha < 1$, were introduced by Lévy (cf. [6], pp. 260-262, or [8], pp. 178-179). After a normalization of the unit of length on the x-axis, the unilateral stable distributions, which will be denoted by $\psi(x) = \psi_\alpha(x)$, where $-\infty < x < \infty$ and $0 < \alpha < 1$, are constant either for $-\infty < x \leqq 0$ or for $0 \leqq x < \infty$, and their Fourier-Stieltjes transforms

$$(4) \qquad \int_{-\infty}^{\infty} e^{iux} d\psi(x), \text{ where } d\psi(x) \geqq 0 \text{ and } \int_{-\infty}^{\infty} d\psi(x) = 1,$$

are identical either with

$$(5) \qquad \exp(-|u|^\alpha[-1 + i \tan(\tfrac{1}{2}\alpha\pi)\operatorname{sgn} u]), \text{ where } -\infty < u < \infty,$$

or with the complex conjugate of (5).

Since both (4) and (5) go over into their complex conjugates if u is replaced by $-u$, it is sufficient to consider the case in which (4) is identical with (5) itself, where $\psi = \psi_\alpha$. Then $d\psi_\alpha(x) = 0$ for $-\infty < u \leqq 0$; hence

$$(6) \qquad \exp(-u^\alpha + iu^\alpha \tan \tfrac{1}{2}\alpha\pi) = \int_0^\infty e^{iux} d\psi_\alpha(x),$$

if, as always from now on, *u is confined to the half-line* $0 \leqq u < \infty$ (this involves no loss, since (4) goes over into its complex conjugate if u is replaced by $-u$).

What will be needed of all of this can be summarized as follows: If $0 < \alpha < 1$, then there exists on the x-half-line $[0,\infty)$ a *monotone* function ψ_α (with $\psi(0) = 0$, $\psi(\infty) = 1$) satisfying (6) on the u-half-line $[0,\infty)$.

4. Change the unit of length on the x-axis in such a way that u becomes replaced by cu, where $c = c_\alpha$ is the positive constant $(\cos \frac{1}{2}\pi\alpha)^{1/\alpha}$, and denote the function of x which thus results from $\psi_\alpha(x)$ again by $\psi_\alpha(x)$. Then $\psi_\alpha(0) = 0$, $\psi_\alpha(\infty) = 1$ and $d\psi_\alpha(x) \geqq 0$ hold again, but (6) becomes simply

$$(7) \qquad \exp(-iu)^\alpha = \int_0^\infty e^{iux} d\psi_\alpha(x),$$

since the parenthetical expression on the left of (6) becomes replaced by $-a_a u^a + i b_a u^a = (e^{-\frac{1}{2}\pi i} u)^a$, where

$$(8) \qquad a_a = \cos \tfrac{1}{2}\pi a, \qquad b_a = \sin \tfrac{1}{2}\pi a \qquad (0 < a < 1).$$

For every a (< 1), the analytic behavior of $\psi_a(x)$ on $[0, \infty)$ is as follows: $\psi_a(x)$ is (i) of class C^∞ on $[0, \infty)$ and (ii) analytic (regular) at every point $x > 0$ of $[0, \infty)$ but (iii) singular at the end-point, $x = 0$, of $[0, \infty)$, since all derivatives of $\psi_a(x)$ vanish at $x = 0$ (so that the analytic behavior of $\psi_a(x)$ is the same as that of the function which is $\exp(-x^{-1})$ for $x > 0$ and 0 for $x \leqq 0$).

In fact, if a_a and b_a are defined by (8), then $\psi_a'(x) = d\psi_a(x)/dx$ can be represented as the following explicit Laplace transform:

$$(9) \qquad \psi_a'(x) = \frac{1}{\pi} \int_0^\infty e^{-xt} \exp(-a_a t^a) \sin(b_a t^a)\, dt, \text{ where } 0 < x < \infty;$$

cf. [14], p. 128 (where the parameter β is 0 in the present *unilateral* case). Clearly, (ii) is implied by (9). On the other hand, (i) and (iii) can be obtained, after some explicit labor, by letting $x \to +0$ in (9). But it is easier to proceed as follows:

If $\psi_a(x)$ is defined to be 0 for $-\infty < x \leqq 0$, then, on the one hand, the integral (7) becomes (4) and, on the other hand, (i) and (iii) together become equivalent to the statement that $\psi_a(x)$ is of class C^∞ on $(-\infty, \infty)$. But Fourier's inversion formula shows that $\psi(x)$ is certainly of class C^∞ on $(-\infty, \infty)$ if, for every fixed n, the function (4) of u is $O(|u|^{-n})$ as $|u| \to \infty$. Finally, the case (7) of (4) satisfies this O-condition, since the absolute value of the function on the left of (7) is $\exp(-|u|^a)$, where $a > 0$.

5. Since $\psi_a(x)$ is monotone and bounded on the x-half-line $[0, \infty)$, and since (7) is valid on the open u-half-line $(0, \infty)$ (incidentally, at $u = +0$ as well), it is clear, by absolutely-uniform convergence and for reasons of analyticity, that (7) remains valid if $-iu$ is replaced by $-z$, where z is any point of the half-plane $\operatorname{Re} z > 0$. Hence, if z is chosen to be real, it follows that

$$(10) \qquad \exp(-x^a) = \int_0^\infty e^{-xu} d\psi_a(u), \text{ where } d\psi_a(u) \geqq 0, \qquad (0 < a < 1),$$

holds on the open x-half-line $(0, \infty)$ and, for trivial reasons of continuity, on the closure $[0, \infty)$ of $(0, \infty)$ as well.

In view of the Hausdorff-S. Bernstein theorem, the existence of a function ψ_a satisfying (10) on $[0,\infty)$ does not state more than that the n-th derivative of $\exp(-x^a)$ is non-negative or non-positive on $[0,\infty)$ according as n is even or odd; and, since $0 < a < 1$ by assumption, this follows by a trivial induction from n to $n+1$. Conversely, since the steps in the preceding deduction (6) $\Rightarrow$ (7) $\Rightarrow$ (10) can of course be retraced, an application of the existence theorem of Hausdorff-Bernstein, when applied to $\exp(-x^a)$, supplies the existence of Lévy's unilateral stable distributions.*

In any case, (9) supplies the explicit form of the distribution occurring in (10). Actually, (9) will not be used in what follows (although the corollary (ii) of (9) in § 4 will be needed in order to obtain the additional information claimed in the last paragraph of § 2).

6. In order to prove the first italicized assertion of § 2, let a, β be any pair of indices satisfying $0 < a < \beta < \infty$ and let t vary on the half-line $[0,\infty)$. Then (10) is applicable when a and x are replaced by a/β and t respectively. Hence

$$\exp(-t^\gamma) = \int_0^\infty e^{-tu} d\psi_\gamma(u), \text{ where } \gamma = a/\beta. \tag{11}$$

But $[0,\infty)$ goes over into itself if t is replaced by t^c, where c is any positive constant. Choose $c = \beta$. Then, since $\psi_\gamma(0) = 0$, $\psi_\gamma(\infty) = 1$ and $d\psi_\gamma(u) \geqq 0$, it follows from (11), by placing $v = u^{1/\beta}$, that there exists on the v-half-line $[0,\infty)$ a monotone function $\psi(v) = \psi_{a\beta}(v)$ satisfying $\psi(0) = 0$, $\psi(\infty) = 1$ and

$$\exp(-t^a) = \int_0^\infty \exp\{-(tv)^\beta\}\, d\psi_{a\beta}(v), \tag{12}$$

---

* It is clear that the formal fact used above can be phrased more generally, as follows: If $d\mu(u)$ is a *symmetric* distribution on $(-\infty,\infty)$ and $F(t) = F(-t)$ denotes its characteristic functon (i. e., the integral of $\exp(ixu)\,d\mu(u)$ or $\cos(xu)\,d\mu(u)$ over $(-\infty,\infty)$ for a fixed real t, where $d\mu(u) + d\mu(-u) = 0$, $d\mu(u) \geqq 0$ and $F(0) = 1$), and if $F(t)$ is totally monotone for positive t, then $F(i\,|\,t\,|\operatorname{sgn} t)$ is the characteristic function of a certain *unilateral* distribution $d\lambda(u) \geqq 0$ on $(-\infty,\infty)$, with $d\lambda(u) = 0$ on $(-\infty,0)$, and vice versa. For, by the Hausdorff-Bernstein theorem, the total monotony of $F(t)$ means the existence of a distribution $d\lambda(u)$ on $[0,\infty)$ for which the integral of $\exp(-tu)\,d\lambda(u)$ over $[0,\infty)$ becomes $F(t)$ at every $t > 0$.

The symmetry of the original distribution $d\mu(u)$ on $(-\infty,\infty)$ is implied, of course, by the circumstance that its characteristic function $F(t)$ is real-valued (hence, even). The introduction of Hausdorff-Bernstein transforms into the theory of probability is due to P. Lévy; cf., e. g., his note in the *Comptes Rendus*, vol. 207 (1938), pp. 1368-1370, where these transforms occur in connection with certain (more general than stable) distribution laws of indefinite divisibility.

where $0 \leqq t < \infty$ and

$$(13) \qquad \int_0^\infty | d\psi_{\alpha\beta}(v) | = \int_0^\infty d\psi_{\alpha\beta}(v) = 1 < \infty.$$

Let $x \geqq 0$, multiply (12) by $\cos(xt)$, and integrate the product over the half-line $0 \leqq t < \infty$ (while x is fixed). It is seen from the definition (1) that what then results differs from the assertion (2) only in notation, provided that it is legitimate to interchange the order of integrations with respect to t and v. Finally, it is clear from (13) and from the parenthetical remark made after (1) that the legitimacy of this interchange is assured by Fubini's theorem.

The proof of the stratification theorem (2) of Cauchy's transcendents (1) is now complete. The explicit form of the derivative of the (absolutely continuous) function $\phi_{\alpha\beta}(u)$ occurring in (2) follows from (9) and from the substitutions which lead from (11) and (12) to (12) and (2) respectively.

7. Let finally be mentioned a simple proof of the fact that $F_\alpha(x) \geqq 0$ cannot hold for all $x > 0$ if $\alpha > 2$.

If α is arbitrary (> 0), it follows from the parenthetical remark made after (1) that, if F_α is denoted by F, the integral

$$(14) \qquad \int_0^\infty F(x) \cos tx \, dx$$

is absolutely convergent (at $t = 0$ and, therefore, at every t). On the other hand, (14) is the Fourier inversion of (1) and is therefore identical with $\exp(-t^\alpha)$, where $0 \leqq t < \infty$. But the latter function is $1 + O(t^\alpha)$, as $t \to 0$, for every $\alpha > 0$; hence, it is $1 + o(t^2)$ if $\alpha > 2$.

Consequently, it is sufficient to ascertain that if $F(x)$ is any function which is absolutely integrable on the half-line $0 \leqq x < \infty$ and which has the property that the corresponding function (14) is $1 + o(t^2)$ as $t \to 0$, then, unless $F(x)$ vanishes identically, $F(x) \geqq 0$ cannot hold for all x. But this can be seen as follows (cf., e. g., [12], p. 33):

Since (15) is a continuous function of t and is $1 + o(t^2)$ as $t \to 0$, it follows, by placing $t = 0$ in (14) and subtracting the result from (14) itself, that

$$\int_0^R F(x) \sin^2(\tfrac{1}{2}tx) \, dx = o(t^2), \text{ where } t \to 0,$$

holds for $R = \infty$ and therefore, if $F(x) \geqq 0$ throughout, for any positive function $R = R(t) < \infty$. Since $\sin^2 u$ exceeds a positive constant multiple of u^2 if $0 \leqq u \leqq \frac{1}{2}$, it follows, by choosing $R(t) = 1/t$, that, as $t \rightarrow 0$,

$$\int_0^{1/t} F(x)(tx)^2 dx = o(t^2), \text{ hence } \int_0^{1/t} F(x)x^2\,dx = o(1),$$

and so $\int_0^\infty F(x)x^2 dx = 0$. Since $F(x) \geqq 0$, this proves the identical vanishing of F (for almost all x).

8. The proof of (2) depended on the formal steps (6) $\Rightarrow$ (7) $\Rightarrow$ (10) $\Rightarrow$ (2) and rested, therefore, on the following fact (cf. the second paragraph of § 5): If $f_\alpha(x) = \exp(-x^\alpha)$, where $0 \leqq x < \infty$, then there exists for $0 \leqq u < \infty$ one monotone function $\phi_{\alpha\beta}(u)$ for which

$$(*) \qquad f_\alpha(x) = \int_0^\infty f_\beta(xu)\,d\phi_{\alpha\beta}(u), \text{ where } d\phi_{\alpha\beta}(u) \geqq 0,$$

is an identity in x, where α and β are arbitrary parameters satisfying $0 < \alpha < \beta < \infty$. Instances of such a stratification rule (*) which are more on the surface than is its instance $f_\alpha(x) = \exp(-x^\alpha)$ are $f_\alpha = g_\alpha$ and $f_\alpha = h_\alpha$, where $g_\alpha(x)$ denotes $(1+x)^{-\alpha}$, while $h_\alpha(x)$ denotes $(1-x)^{\alpha-1}$ or 0 according as $0 \leqq x < 1$ or $1 \leqq x < \infty$.

First, if $x > 0$ and $\beta > \alpha > 0$, then the integral of $(x+u)^{-\beta}u^{-1+\beta-\alpha}$ over the u-half-line $[0,\infty)$ is convergent and (as seen by placing $u = xv$ at a fixed x) has a value which is independent of x (the value of this positive constant $C = C(\alpha,\beta)$ follows from one of the definitions of the beta-function). Hence, if x and u are replaced by $x+1$ and $u-1$ respectively, it follows that

$$(1+x)^{-\alpha} = c_{\alpha\beta} \int_1^\infty (u+x)^{-\beta}(u-1)^{-1+\beta}du, \text{ where } c_{\alpha\beta} > 0,$$

holds on the open x-half-line $(-1,\infty)$ and so, in particular, on $[0,\infty)$. The satisfaction of (*) on $[0,\infty)$ by $f_\alpha = g_\alpha$, where $g_\alpha(x) = (1+x)^{-\alpha}$, now follows if u is replaced by $1/u$ in the last integral (so that $d\phi_{\alpha\beta}(u) = 0$ in (*) if $1 \leqq u < \infty$).

Clearly, the satisfaction of (*) by $f_\alpha = h_\alpha$ can be verified in the same way.

9. It is clear that if (*) is satisfied by a family $f_\alpha(x)$, then it is also satisfied (I) by the family $f_\alpha(x^\mu)$, where μ is any positive constant, and (II) by the family

$$\int_0^\infty k(xs) f_\alpha(s)\, ds,$$

where $k(t)$ is an "arbitrary" function of $t (\geqq 0)$, subject (relative to f_α) to the applicability of Fubini's theorem.

For instance, (2) resulted by choosing $f_\alpha(x) = \exp(-x^\alpha)$ and $k(t) = \cos t$ in (II). But $k(t) = \sin t$ (or, more generally, $k(t) = t^\gamma Z(t)$, where $Z(t)$ is a cylindrical function, such as $J_\lambda(t)$ or $K_\lambda(t)$, and γ an appropriate index, leading to the applicability of Fubini's theorem) could also have been allowed. Thus (2) remains true if $\cos xt$ is replaced by $\sin xt$ in (1).

In order to illustrate (II) *and* (I), apply first (I) alone, by choosing in it $\mu = 2$ and either $f_\alpha = g_\alpha$ or $f_\alpha = h_\alpha$, where g_α, h_α are the functions of § 8. It then follows that (*) holds for $f_\alpha(x) = (1 + x^2)^{-\alpha-\frac{1}{2}}$, where $0 \leqq x < \infty$, as well as for the function $f_\alpha(x)$ which is $(1 - x^2)^{\alpha-\frac{1}{2}}$ or 0 according as $0 \leqq x < 1$ or $1 \leqq x < \infty$ (in both cases, $0 < \alpha < \infty$). Hence, if (II) is applied to $k(t) = \cos t$ in both cases, the "real integral" definition of the cylindrical functions $J_\lambda(t)$, $K_\lambda(t)$ shows that (*) holds, if $\beta > \alpha > 0$, for $f_\alpha(x) = J_{\alpha-\frac{1}{2}}(x)/x^{\alpha-\frac{1}{2}}$ and $f_\alpha(x) = K_{\alpha-\frac{1}{2}}(x)/x^{\alpha-\frac{1}{2}}$ and, therefore (with some $\phi_{\alpha\beta}$), for $f_\alpha = J_{\alpha-\frac{1}{2}}$ and $f_\alpha = K_{\alpha-\frac{1}{2}}$ and so, in particular, for $f_\alpha = J_\alpha$ and $f_\alpha = K_\alpha$.

* * *

10. Corresponding to the stratification theorem (2) of Cauchy's transcendents (1), where α (> 0) is arbitrary, there is (in terms of some family of distribution ϕ) a stratification theorem

$$E_\alpha(z) = \int_0^\infty E_\beta(zu)\, d\phi_{\alpha\beta}(u), \qquad (d\phi_{\alpha\beta}(u) \geqq 0), \tag{15}$$

where $E_\alpha(z)$ denotes Mittag-Leffler's entire function

$$E_\alpha(z) = \sum_{n=0}^\infty z^n / \Gamma(1 + \alpha n) \tag{16}$$

and z can be complex in (15): *If* $0 < \alpha < \beta < \infty$, *then there exists on the half-line* $0 \leqq u < \infty$ *a monotone function* $\phi(u) = \phi_{\alpha\beta}(u)$ *satisfying* $\phi(0) = 0$, $\phi(\infty) = 1$ *and* (15).

The (absolute) convergence of the integral (15) at every point z of the complex plane is part of the assertion. The proof can be based on the following fact, verified in [15] along the lines of pp. 61-64 of my paper in vol. 58 (1936) of this Journal: Corresponding to every index θ on the range $0 < \theta < 1$, there exists on the line $-\infty < t < \infty$ a monotone function $\psi(t) = \psi_\theta(t)$ in terms of which the identity

$$(17) \qquad \Gamma(z+1)/\Gamma(\theta z+1) = \int_{-\infty}^{\infty} e^{-zt} d\psi_\theta(t) \qquad (d\psi_\theta(t) \geqq 0)$$

holds on the half-plane $\operatorname{Re} z > -1$ and so, in particular, on the half-line $z \geqq 0$.

Choose $z = \beta x$, where $\beta > 0$ and $x \geqq 0$, put $\alpha = \theta\beta$, and replace t by $-\log s$ in (17). Then, if $-\psi_\theta(-\log s)$ is denoted by $\phi(s)$, where $0 < s < \infty$, it is seen that, whenever $0 < \alpha < \beta$ (i. e., $0 < \theta < 1$ for $\theta = \alpha/\beta$), the relation

$$\Gamma(\beta x + 1)/\Gamma(\alpha x + 1) = \int_0^\infty s^x \, d\phi(s), \text{ where } 0 \leqq x < \infty,$$

holds for a certain monotone function $\phi(s) = \phi_{\alpha\beta}(s)$ satisfying $\phi(0) = \phi(+0) = 0$ and $\phi(\infty) = 1$ (in fact, the gamma-quotient on the left becomes 1 at $x = 0$). If x and s are now replaced by n and u respectively, it follows that *the Stieltjes moment problem*

$$(18) \qquad \int_0^\infty u^n \, d\phi_{\alpha\beta}(u) = \Gamma(\beta n + 1)/\Gamma(\alpha n + 1) \qquad (n = 0, 1, \cdots)$$

has a solution $d\phi_{\alpha\beta}(u) \geqq 0$ *whenever* $\beta > \alpha > 0$.

Since all coefficients of (16) are positive, it is sufficient to prove (15) for positive z. But then a term-by-term integration (at *this* stage, possibly with the result $\infty = \infty$) is allowed in what results if (16), with α and z (> 0) replaced by ψ and zu respectively, is inserted on the right of (15). Hence (15) is equivalent to

$$(19) \qquad E_\alpha(z) = \sum_{n=0}^{\infty} z^n \int_0^\infty u^n d\phi_{\alpha\beta}(u).$$

Since the truth of (19) is clear from (18) and (16), the proof is complete.

The simplest particular case of the general stratification theorem of (16), a particular case to which (16) cannot be reduced directly, is a result of W. Feller (found by him by entirely different means, namely, by an appeal to Lévy's result on the case $\alpha < 2$ of (1); cf. [10]), which states that $E_\gamma(-x)$ is totally monotone on $[0, \infty)$ if $0 < \gamma < 1$ (and, of course, if $\gamma = 1$). This fact relates to (15) in about the same way as (10) relates to (2). In order to see this, replace α, β and z in (15) by γ, 1 $(> \gamma > 0)$ and $-x$ respectively, and denote the case $\alpha = \gamma$, $\beta = 1$ of $\phi_{\alpha\beta}$ by ϕ_γ. Then (15) goes over into

$$(20) \qquad E_\gamma(-x) = \int_0^\infty e^{-xu} d\phi_\gamma(u), \qquad (0 < \gamma < 1),$$

since $E_1(z) = e^z$, by (16). Since $d\phi_\gamma(u) \geqq 0$, and since (20) holds for every x, it follow from (20) that $E_\gamma(-x)$ is totally monotone on $(-\infty, \infty)$ or, equivalently, on $[0, \infty)$. If x is replaced by $-x$ in (16), this can be formulated as follows: *If* $0 < \gamma < 1$, *then* $E_\gamma(x)$ *and all of its derivatives are positive for* $-\infty < x < \infty$ (this is clear from (16) only for $0 \leqq x < \infty$ but then, of course, for every $\gamma = \alpha > 0$).

Remark. There results a stratification theorem corresponding to (2) and (16) if Cauchy's and Mittag-Leffler's transcendents, (1) and (16), are replaced by the entire function

$$(21) \qquad e_\alpha(z) = \sum_{n=0}^{\infty} z^n / \Gamma(\alpha + n),$$

considered (in a slightly different form) by Euler and (precisely in this form) in Heaviside's formal work on fractional differentiation (for $0 < \alpha < 1$ and, more particularly, for $\alpha = \frac{1}{2}$).

Both (16) and (21) reduce to e^z if $\alpha = 1$. But it so happens that *the proviso* $0 < \alpha < \beta$ *of* (15) *must be changed to* $0 < \beta < \alpha$ *if* (16) *is replaced by* (21). In other words, corresponding to every pair of indices satisfying $0 < \alpha < \beta$, there exists on the half-line $0 \leqq u < \infty$ a function $\phi(u) = \phi_{\alpha\beta}(u)$ for which

$$(22) \qquad e_\beta(z) = \int_0^\infty e_\alpha(zu) d\phi_{\alpha\beta}(u), \text{ where } \phi_{\alpha\beta}(0) = 0,\ \phi_{\alpha\beta}(\infty) = 1 \text{ and } d\phi_{\alpha\beta}(u) \geqq 0,$$

holds as an identity in z.

This counterpart of (15) lies quite on the surface. In fact, instead of (18), only the definition,

$$(23) \qquad \int_0^1 u^{s-1}(1-u)^{t-1} du = \Gamma(s)\Gamma(t)/\Gamma(s+t), \qquad (s > 0, t > 0),$$

of the beta-function is now needed. In addition, $d\phi_{\alpha\beta}(u)=0$ for $1<u<\infty$ in (22), and the existence statement of (22) can be replaced by the explicit formula

$$(24)\qquad \Gamma(\beta-\alpha)e_\beta(z)=\int_0^1 e_\alpha(zu)u^{\alpha-1}(1-u)^{\beta-\alpha-1}du,$$

where $0<\alpha<\beta<\infty$. For, if the definition (21) is inserted on the right as well as on the left of (24), comparison of like powers of z shows that (24) is equivalent to what results if (23) is applied as follows: $s=\alpha+n$ and $t=\beta-\alpha$, where $n=0,1,\cdots$ (so that, since $0<\alpha<\beta$, the parenthetical proviso of (23) is satisfied for every $n\geqq 0$).

APPENDIX.

On a theorem of F. Bernstein.

Let s be a positive constant (to play the part of a standard deviation or of its reciprocal value) and put $\epsilon(x)=\exp(-x^2)$. Then, since (1) reduces to a constant multiple of an $\epsilon(sx)$ if $\alpha=2$, it is clear from the case $\beta=2$ of (2) that Lévy's theorem, asserting the positivity of $F_\alpha(x)$ when $\alpha<2$, is equivalent to the statement that, if $G(t)=G_s(t)$ denotes, for a fixed $x>0$, the "Gauss-Fourier transform"

$$(1)\qquad G(t)=\int_0^\infty \cos(tx)\epsilon(sx)g(x)dx,\ \text{where } \epsilon(y)=\exp(-y^2),$$

of a function $g(x)$, where $0\leqq x<\infty$, then

$$(2)\qquad G(t)>0,\ \text{where } 0\leqq t<\infty$$

(or, equivalently, $-\infty<t<\infty$), holds for a certain $g=g_\alpha$ (if $0<\alpha<2$).

Quite another class of functions g for which (*1*) satisfies (*2*) (for every $s>0$) was considered by F. Bernstein [*1*] (cf. also Mathias' subsequent paper [*2*]; in particular, his Satz 13). Starting with a certain expansion of an "arbitrary" $g(x)$, subject to restrictions of integrability (and, for some reason, of analyticity) of the functions occurring in the expansion, he considers a "Hankel kernel" $K(x,y)$, a kernel which is a function $K(x+y)$ of $x+y$ alone; and, in terms of certain properties (in this connection, cf. [*3*], pp. 328-329) of a bilinear expansion of $K(x+y)=g(x+y)$, he specifies a condition under which (*1*) will satisfy (*2*). Finally, by an application of the addition theorem of elliptic functions to $K(x+y)=\operatorname{cn}(x+y)$, Bernstein proves that his conditions are fulfilled, hence (*2*) holds for (*1*), if

$$(3) \qquad g(x)=\operatorname{cn} x, \text{ where } \operatorname{cn} x=\operatorname{cn}(x,k) \text{ and}^{*}\ 0 \leqq k < 1$$

(this Jacobian elliptic function $g(x)=g_k(x)$ is real-valued, even and periodic, with a period $T=T(k)$ which tends to 2π as $k \rightarrow 0$ and to ∞ as $k \rightarrow 1$).

It does not seem to have been observed in the literature that this result of Bernstein has actually little to do either with his bilinear expansions or with such a specific matter as the addition theorem of elliptic functions. In fact, it so happens that (*2*) must be satisfied by (*1*) whenever (i) the function $g(x)$ is continuous, even, periodic (of an arbitrary period T) and such that $a_n \geqq 0$ holds for every n, and $a_n > 0$ for some n, in its Fourier series

$$(4) \qquad g(x) \sim \sum_{n=0}^{\infty} a_n \cos(2\pi n x/T) = g(x), \text{ where } 0 = \sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} | a_n | < \infty ;$$

more generally, whenever (ii) there exists on the half-line $0 \leqq \lambda < \infty$ a monotone function $f(\lambda)$ satisfying

$$(5) \quad g(x) = \int_0^{\infty} \cos(\lambda x)\, df(\lambda), \text{ where } 0 < f(\infty) - f(0) = \int_0^{\infty} | df(\lambda) | < \infty .$$

Bernstein's result on (*3*) follows from (i), since the classical Fourier series (Jacobi; cf. e. g., [*3*], p. 330) of (*3*) puts into evidence the truth of $a_n \geqq 0$ in the case (*3*) of (*4*). [In this connection, it is worth mentioning that also the results of Stieltjes ([*4*], pp. 549-555; cf [*3*], pp. 329-330) on the Laplace transform of (*3*) and a corresponding Stieltjes transform depend merely on the satisfaction of the assumption $a_n \geqq 0$ of (*4*) by (*3*).]

Curiously enough, the trivial limiting case $k=0$ of Bernstein's result on (*3*), the case in which (*3*) and the assertion (*2*) for (*1*) reduce to $g(x)=\cos x$ and

$$(6) \qquad \int_0^{\infty} \cos(tx) \exp(-sx^2) \cos x \, dx > 0 \qquad (s > 0)$$

respectively, is sufficient in order to prove not only the generalization (i) of Bernstein's result but even the generalization (ii) of (i).

---

[*] Actually, the limiting case $k=1$ need not be excluded. This follows either for reasons of continuity or, more directly, by observing that, on the one hand, $\operatorname{cn}(x,k) = 1/\cosh x$ if $k=1$, and, on the other hand, the value of $G(x)$ is known to be given by an explicit cosh-formula, rendering $G(x) > 0$ trivial, if $g(x) = 1/\cosh x$.

In fact, it is clear from reasons of distributivity that, in order to prove (ii), it is sufficient to verify the satisfaction of (*2*) by (*1*) for the case in which the function $f(\lambda)$ occurring in (*5*) is a step-function consisting of a single saltus (> 0, which can be assumed to be 1). But (*2*) then becomes equivalent to what results when the second cosine is replaced by $\cos(\lambda_0 x)$ in (*6*), where $f(\lambda) = \frac{1}{2}\operatorname{sgn}(\lambda - \lambda_0)$. After a change of the unit of length on the x-axis in (*6*), this can be reduced to the two particular cases $\lambda_0 = 0$, $\lambda_0 = 1$. If $\lambda_0 = 0$, then, since $\exp(-\frac{1}{2}t^2)$ is its own Fourier (cosine) reciprocal, $G(t)$ becomes $a\exp(-bt^2)$, where $a > 0$ and $b \geqq 0$ are constants; so that (*2*) is true if $\lambda_0 = 0$. If $\lambda_0 = 1$, then $G(t)$ is the integral (*6*) (as it stands now). Finally, the truth of the inequality (*6*) need not be concluded from the case $k = 0$ of Bernstein's result on (*3*). In fact, an application of the limiting case ($\cos(\alpha \pm \beta) = \cdots$; $k = 0$) of the addition theorem of the elliptic function (*3*) shows that the integral (*6*) can be written as the sum of two functions of the form $a\exp(-bt^2)$, where $a > 0$, $b \geqq 0$.

What all of this actually verifies is nothing but the fact that, under the assumption (*5*) of (iii), the function (*1*), instead of satisfying just (*2*), is a totally monotone function of $t^{\frac{1}{2}}$, where $0 \leqq t < \infty$. In particular, $G(t)$ is a decreasing function (unless $G(t) =$ Const., i. e., unless $f(\lambda) =$ const. $\operatorname{sgn}\lambda$), a fact not revealed by Bernstein's proof (*loc. cit.*) of (*2*) even in his case (*3*).

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] F. Bernstein, "Über das Fourierintegral . . .," *Mathematische Annalen*, vol. 79 (1920), pp. 265-268.

[2] A. Cauchy, *Œuvres complètes*, ser. 1, vol. 12 (1900 [1853]).

[3] E. Czuber, "Die Entwicklung der Wahrscheinlichkeitstheorie und ihrer Anwendungen," *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 7 (1898), pp. 1-271.

[4] F. Y. Edgeworth, "The law of error," *Philosophical Magazine*, ser. 5, vol. 16 (1883), pp. 300-309.

[5] P. Lévy, "Sur les lois stables en calcul des probabilités," *Comptes Rendus*, vol. 176 (1923), pp. 365-366.

[6] ———, *Calcul des probabilités*, Paris, 1925.

[7] ———, *Théorie de l'addition des variables aléatoires*, Paris, 1937.

[8] ———, *Processus stochastiques et mouvement brownien*, Paris, 1948.

[9] P. Pizzetti, *I fondamenti matematici per la critica dei risultati sperimentali*, Genova, 1891.

[10] H. Pollard, "The completely monotonic character of the Mittag-Leffler function $E_a(-x)$," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 1115-1116.

[11] G. Pólya, "On the zeros of an integral function represented by Fourier's integral," *Messenger of Mathematics*, vol. 52 (1923), pp. 185-188.

[12] A. Wintner, *Lectures on Asymptotic Distributions and Infinite Convolutions*, Institute for Advanced Study (Planographed by Edwards Brothers, Inc.), 1938.

[13] ———, "On the shape of the angular case of Cauchy's distribution curves," *Annals of Mathematical Statistics*, vol. 18 (1947), pp. 589-593.

[14] ———, "Stable distributions and Laplace transforms," *Annali della Scuola Normale Superiore di Pisa*, ser. 3, vol. 10 (1956), pp. 127-134.

[15] ———, "On Heaviside's and Mittag-Leffler's generalizations of the exponential function, the symmetric stable distributions of Cauchy-Lévy, and a property of the gamma-function," to appear in the Fréchet jubilee volume of the *Journal de Mathématique* (1958).

APPENDIX.

[*1*] F. Bernstein, "Ein Kriterium für den positiv definiten Charakter von Fourierintegralen und die Darstellung solcher als Summe von Quadraten," *Mathematische Annalen*, vol. 85 (1922), pp. 155-159.

[*2*] M. Mathias, "Über positive Fourier-Integrale," *Mathematische Zeitschrift*, vol. 16 (1923), pp. 103-125.

[*3*] O. Perron, *Die Lehre von den Kettenbrüchen*, Leipzig-Berlin, 1913.

[*4*] T. J. Stieltjes, *Œuvres complètes*, vol. 2, Groningen, 1918.

ON COSINE-LIKE ARCHES.*

By AUREL WINTNER.

Let $f(x)$ be a function possessing derivatives of arbitrarily high order on an open x-interval (a,b), and let $(-1)^n D^{2n} f(x) \geqq 0$, where $D = d/dx$, hold on (a,b) for $n = 0, 1, 2, \cdots$. If the trivial case $f(x) = \text{const.}\ (\geqq 0)$ is excluded, then, for reasons of convexity, this infinity of inequalities cannot be satisfied on an unbounded interval (a,b), and so it can be assumed that $(a,b) = (-\frac{1}{2}\pi, \frac{1}{2}\pi)$. The resulting class of functions on the interval

$$(1) \qquad -\tfrac{1}{2}\pi < x < \tfrac{1}{2}\pi$$

will be called *cosine-like*, since $f(x) = \cos x$ is the simplest (non-constant) function satisfying

$$(2) \qquad (-1)^n D^{2n} f(x) \geqq 0 \text{ on } (1) \text{ for } n = 0, 1, \cdots.$$

In fact, (2) means that the graph of each of the functions $f, -D^2 f, D^4 f, -D^6 f, \cdots$ is an arc (over $-\frac{1}{2}\pi < x < \frac{1}{2}\pi$) which is situated in the closure of the upper half-plane (in fact, within the open upper half-plane unless $f(x) = \text{const.} = 0$) and which is (strictly) convex from above.

Correspondingly, a straightforward adaptation of a classical argument (initiated, for the class of continuous convex functions, by Jensen and further developed, for the class of totally monotone functions, by S. Bernstein) shows that, if difference, instead of differential, quotients are used in the definition of the class of cosine-like functions, then the assumption of indefinite differentiability, or even the existence of a first derivative, need not be introduced explicitly.

The general methods of Bernstein also supply, as a corollary, the following information: If $f(x)$ is cosine-like, then it can be continued from the given interval (1) into the z-plane and leads to an entire function $f(z)$ which, in addition, must be of exponential type. Only the first of these two results, proved also by Widder, will be used in what follows. References will be found in the paper of Boas and Pólya, Duke Math. Journ., vol. 9 (1942), pp. 406-407; for an exposition of the relevant results of Bernstein and his successors, cf. Chap. 11 of Boas' *Entire Functions*, New York, 1954.

---

* Received October 8, 1957.

A more delicate (as a matter of fact, a *structural*) function-theoretical information on what is necessary for a cosine-like function is contained in the following theorem:

If a function $f(x)$, *given on* (1), *satisfies* (2), *then there exists on the closed t-interval* $[-1,1]$ *a non-decreasing function* $\phi(t)$ *having the following properties: If* $p(w)$ *denotes the function which is defined by*

$$p(w)=\sum_{n=0}^{\infty}\mu_n w^n, \text{ where } \mu_n=\int_{-1}^{1}t^n d\phi(t) \tag{3}$$

(*hence*, $|\mu_n|\leqq\mu_0$), *on the circle*

$$|w|<1 \tag{4}$$

or, equivalently, by

$$p(w)=\int_{-1}^{1}(1-tw)^{-1}\,d\phi(t) \qquad (d\phi(t)\geqq 0) \tag{5}$$

on the simply-connected domain S which results if both half-lines

$$-\infty<w\leqq-1,\ 1\leqq w<\infty \tag{6}$$

are removed from the w-plane, and if the single-valued, regular function $q(w)$ *is defined on* (4) *or, equivalently, on S, by*

$$q(w)=(1-w^2)^{\frac{1}{2}}p(w), \text{ where } q(0)\geqq 0, \tag{7}$$

then $q(\sin z)$ *is an entire function (of exponential type) of* z *satisfying*

$$f(x)=q(\sin x) \text{ on } (1). \tag{8}$$

The functions $f(x)$ satisfying (8), with (7) and (5) for some $\phi(t)$, and rendering $q(\sin z)$ an entire function,† are not quite so scarce as it might seem from the function-theoretical restrictions needed for (7) and (5), and from Stieltjes' inversion formula of his transform (5) of $d\phi$ (cf., e.g.,

---

† If this restriction, which is essential indeed, is disregarded, then there results a *formal* connection between (7)-(8) and a relation occurring in the theory of orthogonal polynomials. In fact, non-negative functions of the type

$$p(u)=q(u)/\sqrt{(1-u^2)}, \qquad (-1<u<1, \text{ or } u=\sin x),$$

where however $p(u)$ need not satisfy anything like the regularity conditions imposed on it by (5) and the further restriction specified before (8), play there a considerable part, as densities of absolutely continuous weights (cf. Chap. XI-XIII of Szegö's *Orthogonal Polynomials*, New York, 1939; the reason for the formal connection is clear from § 11.5).

§ 43-§ 45 of my *Spektraltheorie*, Leipzig, 1929). For instance, since (2) is satisfied if $f(x) = \cos(vx)$, where v is any value on the interval $0 \leqq v \leqq 1$, it is satified if

$$f(x) = \int_0^1 \cos(vx)\, d\lambda(v), \tag{9}$$

where $\lambda(v)$ is any non-decreasing function. Nor does (2) imply that the entire function $f(z)$ is even (as (9) is). For, since (2) is satisfied by $f(x) = \cos(vx)$ if $0 < v < 1$, it is satisfied by $f(x) = \cos(vx - \beta)$ if $\beta = \beta(v)$ is small enough, and the latter $f(x)$ can be "stratified" (with regard to v) by means of a weight $d\lambda(v) \geqq 0$, as in (9) (and this time for $-1 \leqq v \leqq 1$). But by the theorem to be proved, all these functions $f(x)$ on (1) must be such as to possess a representation (8) in which the corresponding $d\phi(t)$, occurring in (5), satisfies the restrictions implicit in the condition that *the product of* $\cos z$ *and*

$$p(\sin z) = \int_{-1}^{1} (1 - t \sin z)^{-1}\, d\phi(t) \qquad (d\phi(t) \geqq 0) \tag{10}$$

becomes an entire function of z. In this regard, it is instructive to choose $\phi(t) = \frac{1}{2}\operatorname{sgn}(t - t_0)$, where t_0 is any point of the interval $[-1, 1]$. Then $d\phi(t) \geqq 0$ is satisfied. But (10) and (7) show that $f(z) = q(\sin z)$ now becomes the meromorphic function

$$f(z) = W/(1 - t_0 W), \text{ where } W = \sin z \text{ and } -1 \leqq t_0 \leqq 1, \tag{11}$$

a function of z which fails to be an entire function (and, correspondingly, $f(x)$ fails to be cosine-like) unless $t_0 = 0$, hence $f(z) = W = \cos z$. On the other hand, if $\phi(t) = t$, then (10) leads to logarithmic branch-points, instead of poles.*

---

* If $\operatorname{Cn}(x, k)$ denotes what results from Gudermann's $\operatorname{cn}(t, k)$ (i.e., Jacobi's $\cos \operatorname{am} t$), if t is replaced by $2Kx/\pi$, then $y(x) = \operatorname{Cn}(x, k)$, where k is any fixed positive modulus < 1, is the most immediate generalization of $\cos x = \operatorname{Cn}(x, 0)$. But the function $y = y(x) = y_k(x)$, where $y_k = \operatorname{Cn}(x, k)$, though always even, of period 2π, positive on (1) and decreasing on the upper half of (1), must fail to be cosine-like for *every* positive k, since, because of its double periodicity for *complex* x, it has *poles*, except in the limiting case $k = 0$ of $y = \cos x$ itself.

Incidentally, even the case $n = 1$ of (1), instead of being satisfied by $f(x) = \operatorname{Cn}(x, k)$ for every positive $k (< 1)$, is satisfied only for $0 \leqq k \leqq k_0$, where k_0 is an absolute constant which is less than 1. In fact, $y = \operatorname{Cn}(x, k)$ is a *convex* arch over (1) if and only if $q = \exp(-\pi K'/K)$ does not exceed the square-root of $\frac{1}{2}$. This can readily be verified, either by differentiating the logarithmic derivative of Jacobi's

Proof. On (1), let $f(x)$ be a function of class C^∞ satisfying (2). Then $f(x)$ can be extended to an entire function $f(z)$ which, in addition, is of exponential type (S. Bernstein). Even if this additional information is not used, it follows that Taylor's expansion

$$f(x+iy)=\sum_{m=0}^{\infty}(iy)^m D^m f(x)/n! \tag{12}$$

is valid, at every x, for every y. Let x and y be real, and replace the interval (1) by the corresponding strip

$$-\tfrac{1}{2}\pi<\operatorname{Re} z<\tfrac{1}{2}\pi \qquad (z=x+iy). \tag{13}$$

Since the case $n=0$ of (2) implies that $f(z)$ is real for real z, it implies that $2\operatorname{Re} f(z)$ is the sum of $f(x+iy)$ and $f(x-iy)$. Hence, if y is replaced by $-y$ in (12) and if the result is added to (12) itself, it follows that

$$\operatorname{Re} f(z)=\sum_{m=0}^{\infty} y^{2m}(-D^2)^m f(x)/(2m)! \tag{14}$$

holds (by convergence) at every point of the z-plane and so, in particular, on the strip (13). But (14) and (2) imply that

$$\operatorname{Re} f(z)\geqq 0 \text{ on } (13). \tag{15}$$

Accordingly, if $f(x)$ satisfies (2), then it can be extended into an entire function $f(z)$ satisfying (15). Hence, more than what is needed for the completion of the proof is contained in the following criterion (*which does not assure that* $f(z)$ *is an entire function*):

Let $f(z)$ *be a function which is regular on the strip* (13) *and real-valued on the segment* (1), *where* $z=x+iy$. *Then* $f(z)$ *will satisfy* (15) *if and only if there exists on the closed t-interval* $[-1,1]$ *a monotone non-decreasing function* $\phi(t)$ *having the following property: If* $p(w)$ *is defined by the Stieltjes transform* (5) *on the simply-connected w-doman which results when both half-lines* (6) *are removed from the w-plane, then*

$$f(z)=p(\sin z)\cos z \text{ on } (13). \tag{16}$$

This criterion turns out to be a rephrasing of the *symmetric case* of (F. Riesz' version of) the Carathéodory-Toeplitz criterion for functions $F(w)$ which are regular on (4) and satisfy

---

infinite product for $\operatorname{cn}(x,k)$ or by differentiating the pair of rational relations which connect the first derivatives of $\operatorname{cn}(x,k)$ and $\operatorname{sn}(x,k)$ with $\operatorname{sn}(x,k)$ and $\operatorname{cn}(x,k)$ themselves.

$$(17)\qquad \operatorname{Re} F(w) \geqq 0 \text{ on } (4)$$

(by the symmetry restriction is meant the condition

$$(18)\qquad F(w^*) = F^*(w) \text{ on } (4),$$

where the asterisks denote complex conjugations).

Proof. The classical criterion, just mentioned, states that a function $F(w)$ which is regular on (4) will satisfy (17) if and only if there exists on the closed a-interval $[-\pi, \pi]$ a monotone non-decreasing function $\mu(a)$ in terms of which $F(w)$ is representable on (4) in the form

$$(19)\qquad F(w) = \int_{-\pi}^{\pi} L(we^{ia})\, d\mu(a), \text{ where } L(s) = (1+s)/(1-s).$$

In order to characterize those particular distributions $d\mu(a) \geqq 0$ on $[-\pi, \pi]$ for which (19) will satisfy (18), expand (19) according to powers of w on (4) and insert the result in (18). Then comparison of like powers of w shows that (18) is equivalent to

$$2\int_{-\pi}^{\pi} e^{ina}\, d\mu(a) = 2\int_{-\pi}^{\pi} e^{-ina}\, d\mu(a), \text{ i.e., } \int_{-\pi}^{\pi} \sin na\, d\mu(a) = 0,$$

where $n = 1, 2, \cdots$, which in turn is equivalent to the restriction that $d\mu(a) = -d\mu(-a)$ if $0 < a < \pi$. If this is inserted in (19), a trivial reduction leads to

$$(20)\qquad F(w) = \int_{0}^{\pi} P(w, \cos a)\, d\mu(a) \text{ on } (4),$$

where P *is Poisson's kernel*

$$(21)\qquad P(w, \cos a) = (1-w^2)/(1-2w\cos a + w^2)$$

with complex w (instead of the standard $w = |w| = r$) and $\mu(a)$ is monotone non-decreasing on the closed a-interval $[0, \pi]$ but is otherwise arbitrary (the $\mu(a)$ of (20) is not the same as the $\mu(a)$ of (19) was). Thus (20), where $d\mu(a) \geqq 0$ on $[0, \pi]$, is necessary and sufficient in order that a function $F(w)$, regular on (4), be such as to satisfy both (17) and (18).

Let $f(z)$ be a function which is regular on (13), satisfies (15), and is real on (1), where $z = x + iy$. The latter restriction is equivalent to the symmetry assumption

$$(22)\qquad f(z^*) = f^*(z) \text{ on } (13).$$

But it is a standard exercise that

$$(23) \qquad w = \tan \tfrac{1}{2} z$$

is a Riemann mapping function belonging to the strip (14) and the circle (4). Since $(\tan \frac{1}{2} z)^* = \tan(\frac{1}{2} z^*)$, it follows that (17) and (18) are equivalent to (15) and (22) by virtue of $f(z) = F(w)$ and (23). Hence, by the end of the preceding paragraph, the class of functions $f(z)$ dealt with in the last italicized assertion is the class of those functions which are representable on (13) in the form

$$(24) \qquad f(z) = \int_0^\pi P(\tan \tfrac{1}{2} z, \cos a)\, d\mu(a), \text{ where } d\mu(a) \geqq 0.$$

Finally, it is readily verified that, by virtue of (23), Poisson's complex kernel (21) becomes identical with the quotient of $\cos z$ and $1 - t \sin z$, where $t = \cos a$. Hence (24) can be written in the form

$$f(z) = \{ \int_0^\pi (1 - t \sin z)^{-1}\, d\mu(a) \} \cos z,$$

where $t = \cos a$ and $d\mu(a) \geqq 0$. Since this differs from (16) and (5) only in notation, the proof is complete.

Since the crucial formal point in the proof is the explicit simplification which results when (19) is reduced by the symmetry requirement (18), it is worth mentioning that, while the formulation of (19) in terms of the trigonometric moment problem supplied by spectral resolution of arbitrary unitary matrices in Hilbert space (cf., e. g., § 6, of E. Hopf's *Ergodentheorie*, Ergebnisse der Math., vol. 5 (1937), no. 2), the restriction (18) corresponds to the replacement of the unitary group by its orthogonal subgroup (cf. C. R. Putnam and A. Wintner, Amer. Jorn. of Math., vol. 74 (1952), pp. 52-78, and the Johns Hopkins thesis of M. H. Martin referred to there).

THE JOHNS HOPKINS UNIVERSITY.

VECTEURS ANALYTIQUES DANS LES REPRESENTATIONS DE GROUPES DE LIE.*

par P. CARTIER et J. DIXMIER.[1]

Introduction. Soit π une représentation continue[2] du groupe de Lie G dans l'espace de Banach $\mathfrak{H}$. Selon Harish-Chandra [1], on dit qu'un élément $\phi \in \mathfrak{H}$ est un *vecteur analytique* pour la représentation π si l'application $s \rightarrow \pi(s)\phi$ de G dans $\mathfrak{H}$ est analytique. Les vecteurs analytiques de $\mathfrak{H}$ forment un sous-espace vectoriel, non fermé en général, de $\mathfrak{H}$. Lorsque le groupe G est semi-simple et que la représentation π est "permise," Harish-Chandra a démontré dans [1] que les vecteurs analytiques sont partout denses dans $\mathfrak{H}$; nous nous proposons de généraliser ce résultat au cas d'un groupe de Lie quelconque et d'une représentation bornée sur un certain sous-groupe discrét. Le résultat précis est énoncé dans le théorème du § 6, qui est le résultat central de cet article.

Nous suivrons une méthode de démonstration analogue à celle de Harish-Chandra: alors que Harish-Chandra démontrait d'abord que les vecteurs analytiques sont partout denses dans le cas d'une représentation d'un groupe quasi-nilpotent, nous commencerons par une étude approfondie du cas des groupes résolubles; une fois obtenu le résultat pour les groupes résolubles, la démonstration suivra de très près celle de Harish-Chandra.

1. Notations. On désigne par $\boldsymbol{N}$ l'ensemble des entiers $\geqq 0$, par $\boldsymbol{Z}$ celui des entiers rationnels, par $\boldsymbol{R}$ le corps des nombres réels et par $\boldsymbol{C}$ le corps des nombres complexes.

L'élément neutre d'un groupe sera toujours noté e. Si f est une fonction sur un groupe G, la translatée à gauche ${}_sf\,(s \in G)$ est définie par ${}_sf(s') = f(ss')$. La translatée à droite f_s est définie par $f_s(s') = f(s's)$. Sur un groupe localement compact G, une mesure de Haar est une mesure $\geqq 0$ non nulle

---

* Received November 4, 1957.

[1] Les numéros entre crochets renvoient à la Bibliographie située à la fin de l'article.

[2] La représentation π est dite continue si l'application $(x, \phi) \rightarrow \pi(x)\phi$ de $G \times \mathfrak{H}$ dans $\mathfrak{H}$ est continue, ou, ce qui revient au même, si pour tout $\phi \in \mathfrak{H}$, l'application $x \rightarrow \pi(x)\phi$ de G dans $\mathfrak{H}$ est continue.

invariante à gauche; l'élément d'intégrale correspondant sera noté ds si s désigne l'élément générique de G. Une *semi-norme* sur G est une fonction semi-continue inférieurement $\rho > 0$ vérifiant l'inégalité $\rho(ss') \leqq \rho(s)\rho(s')$ pour $s, s' \in G$; pour toute semi-norme ρ on notera $L^p_C(G, \rho)$ l'espace des fonctions numériques complexes sur G de puissance p^e intégrable ($p \geqq 1$) pour la mesure $\rho(s)\,ds$, muni de la norme définie par $\| f \|_{p,\rho} = (\int_G | f(s) |^p \rho(s)\,ds)^{1/p}$; la représentation régulière π de G dans $L^p_C(G, \rho)$ est définie par $\pi(s)f = {}_{s^{-1}}f$ pour $f \in L^p_C(G, \rho)$.

Les espaces de Banach sont toujours supposés complexes (mais il n'y aurait pratiquement rien de changé s'ils étaient supposés réels).

Si $\mathfrak{H}$ est un espace de Banach, on désigne par $\mathscr{L}(\mathfrak{H})$ l'espace de Banach des endomorphismes continus de $\mathfrak{H}$. Si ρ est une semi-norme sur le groupe localement compact G et π une représentation continue de G dans l'espace de Banach $\mathfrak{H}$ telle que $\| \pi(s) \| \leqq \rho(s)$ pour tout $s \in G$, on pose

$$\pi(f) = \int_G f(s)\pi(s)\,ds \quad \in \mathscr{L}(\mathfrak{H})$$

pour $f \in L^1_C(G, \rho)$.

Tous les groupes de Lie envisagés sont supposés réels, sauf mention du contraire.

Soit G un groupe de Lie, d'algèbre de Lie $\mathfrak{g}$; on note exp l'application exponentielle de $\mathfrak{g}$ dans G, et pour toute représentation continue π de G dans un espace vectoriel de dimension finie, on note $d\pi$ la représentation correspondante de $\mathfrak{g}$. On a alors, pour tout $S \in \mathfrak{g}$

$$\pi(\exp S) = \exp d\pi(S) \tag{1}$$

où le second membre est défini comme d'habitude par $\exp T = \sum_{n \geqq 0} T^n/n\,!$,

Soient G_1 et G_2 des sous-groupes de G, on écrira $G = G_1 \cdot G_2$ si et seulement si les conditions suivantes sont remplies:

1) G_1 et G_2 sont des sous-groupes analytiques de G;

2) l'application $(s_1, s_2) \rightarrow s_1 s_2$ de $G_1 \times G_2$ dans G est un isomorphisme de la première variété analytique sur la seconde.

2. Rappel de certains lemmes.

LEMME 1. *Soient E un espace localement compact, μ une mesure $\geqq 0$ sur E, $\mathfrak{H}$ l'espace de Banach des fonctions numériques complexes μ-intégrables, V une variété analytique complexe et f une fonction numérique complexe continue sur $V \times E$ satisfaisant aux conditions suivantes:*

(i) *il existe une fonction μ-intégrable $g \geqq 0$ sur E telle que l'on ait $|f(z,x)| \leqq g(x)$ pour tout $z \in V$ et tout $x \in E$;*

(ii) *pour tout $x \in E$, la fonction $z \to f(z,x)$ est holomorphe sur V.*

Si l'on note alors $\psi(z) \in \mathfrak{H}$ la fonction $x \to f(z,x)$, l'application $z \to \psi(z)$ de V dans $\mathfrak{H}$ est holomorphe.

C'est le lemme 23 de [1].

LEMME 2. *Soient G un groupe de Lie réel, $\mathfrak{H}$ un espace de Banach, π une représentation continue de G dans $\mathfrak{H}$ et ψ un élément de $\mathfrak{H}$. On suppose que l'application $s \to \pi(s)\psi$ est analytique en e; alors le vecteur ψ est analytique pour la représentation π.*

Cf. [1], p. 209, lignes 7-11.

LEMME 3. *Soient G un groupe de Lie réel, $\mathfrak{H}$ un espace de Banach, π une représentation continue de G dans $\mathfrak{H}$. Soit ρ une semi-norme sur G telle que $\|\pi(s)\| \leqq \rho(s)$ pour tout $s \in G$. Alors, si les vecteurs de $L^1{}_C(G,\rho)$ analytiques pour la représentation régulière sont partout denses dans $L^1{}_C(G,\rho)$, les vecteurs de $\mathfrak{H}$ analytiques pour π sont partout denses dans $\mathfrak{H}$.*

Soit A l'ensemble des éléments de $L^1{}_C(G,\rho)$ analytiques pour la représentation régulière. Soit $\mathfrak{K}$ l'ensemble des combinaisons linéaires de vecteurs $\pi(f)x$, où $x \in \mathfrak{H}$ et $f \in A$. Les éléments de $\mathfrak{K}$ sont analytiques pour π ([1], lemme 24), et il suffit de prouver que $\mathfrak{K}$ est partout dense dans $\mathfrak{H}$, autrement dit, que si ϕ est une forme linéaire continue sur $\mathfrak{H}$ nulle sur $\mathfrak{K}$, on a $\phi = 0$. Or, pour toute $f \in A$ et tout $x \in \mathfrak{H}$, on a

$$0 = \phi(\pi(f)x) = \int_G \phi(\pi(s)x)f(s)\,ds = \int_G \phi(\rho(s)^{-1}\pi(s)x)f(s)\rho(s)\,ds.$$

Puisque A est partout dense dans $L^1{}_C(G,\rho)$, on en déduit que $\phi(\rho(s)^{-1}\pi(s)x) = 0$ localement presque partout sur G, donc que $0 = \phi(\pi(e)x) = \phi(x)$ puisque la fonction $s \to \phi(\pi(s)x)$ est continue. D'où notre assertion (cf. aussi [1], lemme 25).

LEMME 4. *Soient X et Y deux variétés analytiques réelles, Y étant compacte, et f une application analytique de $X \times Y$ dans un espace de Banach $\mathfrak{H}$. Tout point de X possède alors un voisinage ouvert V ayant les propriétés suivantes:*

(i) *il existe un système de coordonnées analytiques $(t_1, \cdots, t_n)$ dans V;*

(ii) *il existe des applications analytiques f_e de Y dans $\mathfrak{H}$*

$$(e=(e_1,\cdots,e_n)\in \boldsymbol{N}^n)$$

telles que pour $x\in V$ et $y\in Y$, on ait:

$$f(x,y)=\sum_{e\in \boldsymbol{N}^n} f_e(y)t_1^{e_1}(x)\cdots t_n^{e_n}(x) \tag{2}$$

cette somme étant absolument et uniformément convergente dans $V\times Y$.

Il suffit de reprendre pratiquement sans changement, la démonstration de [1], de la ligne 20 le la p. 221 à la ligne 19 de la p. 222, en remplaçant partout G par X et K par Y.

3. Structure des groupes résolubles. Soient $\mathfrak{h}$ une algèbre de Lie résoluble réelle et $\mathfrak{n}$ un idéal nilpotent de $\mathfrak{h}$ contenant $[\mathfrak{h},\mathfrak{h}]$; on note k la dimension de $\mathfrak{n}$ et n celle de $\mathfrak{h}$. Comme toute algèbre de Lie résoluble contient un idéal de codemnsion 1 et que tout sous-espace de $\mathfrak{h}$ contenant $\mathfrak{n}$ est un idéal de $\mathfrak{h}$, il existe une suite de sous-espaces $\mathfrak{h}_i$ de $\mathfrak{h}$ ayant les propriétés suivantes:

a) $\mathfrak{h}_i$ est de dimension i pour $0\leqq i\leqq n$;

b) $\mathfrak{h}_i$ est un idéal de $\mathfrak{h}_{i+1}$ pour $0\leqq i\leqq n-1$;

c) $\mathfrak{h}_k=\mathfrak{n}$.

La propriété a) nous permet de choisir une base $(X_1,\cdots,X_n)$ de $\mathfrak{h}$ telle que $(X_1,\cdots,X_i)$ soit une base de $\mathfrak{h}_i$. Ces données resteront fixées dans tout ce paragraphe.

LEMME 5. *Il existe un groupe de Lie réel H ayant $\mathfrak{h}$ pour algèbre de Lie et jouissant des propriétés suivantes:*

(i) *l'application $\phi\colon(t_1,\cdots,t_n)\to\prod_{i=1}^{n}\exp t_iX_i$ de $\boldsymbol{R}^n$ dans H est un isomorphisme de variété analytique;*

(ii) *soit $h\to(x_1(h),\cdots,x_n(h))$ l'application réciproque de ϕ et soit A l'algèbre complexe de fonctions sur H engendrée par 1, les x_i $(1\leqq i\leqq n)$ et les $\exp\alpha x_j$ $(\alpha\in\boldsymbol{C},k<j\leqq n)$; pour toute fonction $f\in A$, il existe des fonctions $f_p,f_p'\in A$ telles que l'on ait l'identité:*

$$f(hh')=\sum_{p=1}^{m} f_p(h)f_p'(h'). \tag{3}$$

Nous raisonnerons par récurrence sur n, le cas $n=0$ étant trivial; nous supposerons donc $n>0$ et nous poserons $\mathfrak{h}'=\mathfrak{h}_{n-1}$, $\mathfrak{n}'=\mathfrak{n}\cap\mathfrak{h}'$; la dimension k' de $\mathfrak{n}'$ est égale à $n-1$ si $\mathfrak{n} = \mathfrak{h}$, et est égale à k si $\mathfrak{n} \subset \mathfrak{h}'$; on peut alors construire un groupe de Lie réel H', une application ϕ', une algèbre A' ayant les propriétés (i) et (ii) de l'énoncé, où l'on doit remplacer n par $n-1$ et k par k'.

A) Pour toute fonction $f \in A'$, le sous-espace vectoriel de A' engendré par les translatées à droite de f est de dimension finie sur $\boldsymbol{C}$ d'après la formule (3) ; par suite, A' est réunion de ses sous-espaces de dimension finie invariants par les translations à droite. Soient V' un tel sous-espace et π' la représentation de H' dans V' définie par $\pi'(h) \cdot f = f_h$.

Soit $(f_j)_{1 \leqq j \leqq m}$ une base de V'; d'après la condition (ii) de l'énoncé il existe des fonctions $a_{lj} \in A'$ telles que:

$$\pi'(h) f_l = \sum_{j=1}^{m} a_{lj}(h) f_j \qquad (1 \leqq l \leqq m)\,; \tag{4}$$

mais, si $h = \exp tX_i$ avec $1 \leqq i \leqq k'$, la définition des x_j' montre que $x_j'(h) = 0$ pour $j > k'$ et $x_j'(h) = \delta_{ij} t$ (indice de Kronecker) pour $1 \leqq j \leqq k'$. D'après la définition de A', on voit que pour tout $f \in A'$, $f(\exp tX_i)$ est un polynome en t pour $1 \leqq i \leqq k'$; d'après la formule (4), la matrice de $\pi'(\exp tX_i)$ par rapport à la base (f_j) est donc un polynome en t puisque $a_{lj} \in A'$; mais d'après la formule (1), on a

$$\pi'(\exp tX_i) = \exp d\pi'(tX_i) = \sum_{r \geqq 0} (d\pi'(X_i))^r t^r / r\,!$$

ce qui impose que $d\pi'(X_i)$ soit nilpotent pour $1 \leqq i \leqq k'$.

Soit $(V'_r)_{0 \leqq p \leqq m}$ une suite de Jordan-Hölder de V' pour la représentation π' de H'; d'après le théorème de Lie sur les groupes résolubles, les espaces V_p'/V'_{p-1} sont de dimension 1. Pour $1 \leqq i \leqq k'$, l'opérateur nilpotent $d\pi'(X_i)$ induit un opérateur nul dans V_p'/V'_{p-1}, autrement dit applique V_p' dans V'_{p-1}. Supposons la base (f_j) adaptée à la suite (V_p'), c'est-à-dire que V_p' admet $(f_1, f_2, \cdots, f_p)$ pour base; alors la matrice représentant $d\pi'(X_i)$ est de diagonale nulle pour $1 \leqq i \leqq k'$. Il en résulte que si $Y(u) = X_i + \sum_j u_j X_j$ $(1 \leqq j \leqq k';\ 1 \leqq i \leqq n-1)$, la matrice qui représente $d\pi'(Y(u))$ est triangulaire et que ses termes non diagonaux sont linéaires en $u_1, \cdots, u_{k'}$; si $1 \leqq i \leqq k'$, ses termes diagonaux sont nuls.[2a] Du lemme A de l'Appendice résulte que les coefficients de la matrice associée à l'opérateur $\pi'(\exp tY(u)) = \exp(t d\pi'(Y(u)))$ sont de la forme

$$\sum_{\alpha} E_\alpha(t) P_\alpha(u_1, \cdots, u_{k'}) \tag{5}$$

[2a] On notera que dans vous les cas les termes diagonaux de $d\pi'(Y(u))$ sont indépendants $u_1, \cdots, u_{k'}$.

où les P_α sont des polynomes et où les E_α sont des exponentielles-polynomes[3] *et même des polynomes si $1 \leqq i \leqq k'$.*

Or, de la formule (4) résulte $f_i(h) = \sum_{j=1}^{m} a_{ij}(h) f_j(e)$ et par suite, f_i est de la forme (5) ; comme A' est réunion de sous-espaces analogues à V', on voit que, pour tout $f \in A'$, la fonction

$$(t, u) \to f(\exp t(X_i + \sum_{j=1}^{k'} u_j X_j))$$

est du type (5).

B) Soit D la dérivation $Y \to [X_n, Y]$ de $\mathfrak{h}'$ et soit $\sigma(v)$ l'automorphisme $\exp vD$ de $\mathfrak{h}'$; comme D applique $\mathfrak{h}'$ dans $[\mathfrak{h}, \mathfrak{h}] \cap \mathfrak{h}' \subset \mathfrak{n} \cap \mathfrak{h}' = \mathfrak{n}'$, on a $\sigma(v) \cdot Y - Y \in \mathfrak{n}'$ pour tout $Y \in \mathfrak{h}'$, et les coefficients de $\sigma(v) \cdot Y - Y$ par rapport à la base $(X_1, \cdots, X_{k'})$ de $\mathfrak{n}'$ sont des exponentielles-polynomes en v et même des polynomes si $\mathfrak{n} = \mathfrak{h}$.[3a] De ce qu'on a démontré en A), il résulte alors que pour toute fonction $f \in A'$, la fonction $(t_i, v) \to f(\exp t_i \sigma(v) \cdot X_i)$ est de la forme:

$$(6) \qquad \sum_\alpha E_\alpha(t_i) E_\alpha'(v)$$

où les E_α sont des exponentielles-polynomes et même des polynomes si $1 \leqq i \leqq k'$, tandis que les E_α' sont des exponentielles-polynomes et même des polynomes si $\mathfrak{n} = \mathfrak{h}$.

Soit $\tau(v)$ l'automorphisme du groupe simplement connexe H' associé à l'automorphisme $\sigma(v)$ de $\mathfrak{h}'$; pour $h = \prod_{i=1}^{n-1} \exp t_i X_i$, on a:

$$(7) \qquad \tau(v) \cdot h = \prod_{i=1}^{n-1} \exp t_i \sigma(v) \cdot X_i.$$

De la définition de A', de la formule (6) et de la formule analogue à la formule (3) pour $n-1$ facteurs (que se déduit de (3) par récurrence immédiate), on déduit finalement que, *pour toute fonction $f \in A'$, la fonction $(h, v) \to f(\tau(v) \cdot h)$ est de la forme:*

$$(8) \qquad \sum_\alpha E_\alpha(v) f_\alpha(h)$$

où $f_\alpha \in A'$ et les E_α sont des exponentielles-polynomes. Si $k = n$ (c'est-à-dire $\mathfrak{n} = \mathfrak{h}$), *les E_α sont même des polynomes.*

---

[3] On appelle exponentielle-polynome à p variables $u_1, \cdots, u_p$ réelles ou complexes, une fonction de la forme: $\sum_i P_i(u_1, \cdots, u_p) \exp \sum_j a_{i,j} u_j$ où les P_i sont des polynomes à coefficients complexes et les $a_{i,j}$ des constantes complexes.

[3a] On notera que dans ce dernier cas, la dérivation D est nilpotente.

C) On peut maintenant former le produit semi-direct H de H' et $\boldsymbol{R}$ au moyen du groupe à un paramètre $\tau(v)$ d'automorphismes de H'. On rappelle que ce produit semi-direct est, en tant que variété, identique à $H'\times\boldsymbol{R}$ et que la loi de groupe est donnée par:

$$(h,v)(h',v')=(h\cdot\tau(v)(h'),v+v'). \tag{9}$$

Si l'on identifie X_n au générateur infinitésimal du groupe à un paramètre $v\to(e,v)$ de H, on voit immédiatement que $\mathfrak{h}$ s'identifie à l'algèbre de Lie de H, H' étant identifié au groupe des (h,e).

On a alors:

$$\phi(t_1,\cdots,t_n)=(\phi'(t_1,\cdots,t_{n-1}),e)(e,t_n)=(\phi'(t_1,\cdots,t_{n-1}),t_n)$$

ce qui prouve que ϕ est un isomorphisme de variété analytique. De plus, d'après la définition des x_i, on a:

$$x_i(h,v)=x_i'(h),\quad 1\leqq i<n;\qquad x_n(h,v)=v$$

et par suite A est l'ensemble des fonctions de la forme (8) (où les E_α sont des exponentielles-polynomes en général, des polynomes si $\mathfrak{h}=\mathfrak{n}$). La formule (3) pour $f\in A$ résulte alors immédiatement de la définition de la loi de composition dans H (cf. (9)) et de la conclusion de B).—c. q. f. d.

Nous allons, en vue de besoins ultérieurs, déterminer la mesure de Haar sur le groupe H. L'automorphisme $\tau(v)$ de H' transforme une mesure de Haar μ sur H' en $\Delta(v)\mu$, où $\Delta(v)$ est le déterminant de l'automorphisme contragrédient de $\sigma(v)$; on a donc

$$\Delta(v)=(\det\sigma(v))^{-1}=\exp-vTr(D).$$

Si ν est la mesure de Haar usuelle sur $\boldsymbol{R}$, la formule (9) montre que la translation à gauche par (h,v) transforme la mesure μ en la mesure $\Delta(v)\mu\otimes\nu$; la mesure $\Delta(v)\,d\mu(h)\,d\nu(v)$ est donc une mesure de Haar sur H. Raisonnant par récurrence sur n, on voit que la mesure de Haar sur H est $\exp(\alpha_{k+1}x_{k+1}+\cdots+\alpha_n x_n)\,dx_1\cdots dx_n$ en posant $\alpha_i=-\mathrm{Tr}(\mathrm{ad}\,X_i)$.

4. Vecteurs analytiques. Cas des groupes résolubles.

LEMME 6. *Soit N un groupe de Lie réel résoluble, connexe et simplement connexe. Soit ρ une semi-norme sur N. Les vecteurs de $L^1{}_C(N,\rho)$ analytiques pour la représentation régulière sont partout denses dans $L^1{}_C(N,\rho)$.*

A) Comme deux groupes de Lie connexes et simplement connexes ayant des algèbres de Lie isomorphes sont isomorphes, on peut d'après le lemme 5 trouver des fonctions $x_1,\cdots,x_n$ sur N ayant les propriétés suivantes:

a) l'application $h \rightarrow (x_1(h), \cdots, x_n(h))$ de N dans $\boldsymbol{R}^n$ est un isomorphisme de variété analytique;

b) il existe des exponentielles-polynomes P_i telles que:

$$(10) \quad x_i(hh') = P_i(x_1(h), \cdots, x_n(h)\,;\ x_1(h'), \cdots, x_n(h')) \qquad (1 \leqq i \leqq n)\,;$$

c) la mesure de Haar sur N est de la forme $(\exp \sum \alpha_i x_i)\, dx_1 \cdots dx_n$. De plus, comme d'après (3) l'algèbre A du lemme 5 est réunion de ses sous-espaces de dimension finie invariants par les translations à gauche, on peut trouver des fonctions *réelles* y_j et a_{jk} $(1 \leqq j, k \leqq m)$ sur N, s'exprimant comme exponentielles-polynomes en les x_i et telles que:

d) $m \geqq n$ et $x_j = y_j$ pour $1 \leqq j \leqq n$;

e) on ait les identités:

$$(11) \qquad y_j(hh') = \sum_{k=1}^{m} a_{jk}(h) y_k(h').$$

Comme les exponentielles-polynomes se prolongent en des fonctions entières de variables complexes, on peut d'après le principe du prolongement des identités, plonger N dans un groupe de Lie complexe N^c, les fonctions x_i, y_j et a_{jk} se prolongeant en des fonctions holomorphes sur N^c de sorte que les x_i forment un système de coordonnées complexes sur N^c et que les identités (10) et (11) soient valables sur N^c.

Enfin, pour achever ces préliminaires, notons que sur $\boldsymbol{R}$, toute semi-norme est majorée par une exponentielle: $\rho(x) \leqq M \exp A\,|x|$ $(M, A \in \boldsymbol{R})$ (cf. par exemple [2], chap. VI). Revenant à la définition des x_i (lemme 5) et utilisant l'inégalité $\rho(\prod_{i=1}^{n} \exp t_i X_i) \leqq \prod_{i=1}^{n} \rho(\exp t_i X_i)$ on déduit la majoration:

$$(12) \qquad \rho(h) \leqq M \exp A \sum_{i=1}^{n} |x_i(h)|, \qquad (h \in N)$$

pour une constante réelle A convenable et $M > 0$.

B) Soient $\mathfrak{Q}^c$ l'espace vectoriel complexe des formes quadratiques en des variables $Y_1, \cdots, Y_m$ à coefficients complexes, $\mathfrak{Q}$ le sous-espace réel formé des formes quadratiques à coefficients réels et $\mathfrak{Q}^+$ le cône ouvert de $\mathfrak{Q}$ formé des formes quadratiques positives et non dégénérées. Nous définirons une représentation holomorphe du groupe opposé au groupe complexe N^c dans $\mathfrak{Q}^c$ en posant:

$$(13) \quad (\pi(h)F)(Y_1, \cdots, Y_m) = F(\sum_k a_{1k}(h) Y_k, \cdots, \sum_k a_{mk}(h) Y_k)$$

pour $F \in \mathfrak{Q}^c$ et $h \in N^c$.

Comme $\mathfrak{Q}^+$ est ouvert dans $\mathfrak{Q}$, pour h appartenant à un certain voisinage ouvert V de e dans N^c et $F \in \mathfrak{Q}^+$, la forme $\mathfrak{R}(\pi(h)F) - \frac{1}{2}F$ appartient à $\mathfrak{Q}^+$ ($\mathfrak{R}$ désignant la partie réelle). On en déduit, pour $h \in V$, l'inégalité:

$$\mathfrak{R}F({}_h(y_1), \cdots, {}_h(y_m)) \geqq \tfrac{1}{2}F(y_1, \cdots, y_m)$$

d'où, si $f = \exp - F(y_1, \cdots, y_m)$:

$$|{}_hf| = \exp - \mathfrak{R}F({}_h(y_1), \cdots, {}_h(y_m)) \leqq \exp - \tfrac{1}{2}F(y_1, \cdots, y_m).$$

Or, puisque $F \in \mathfrak{Q}^+$, il existe une constante réelle $\alpha > 0$ telle que la forme $F(Y_1, \cdots, Y_m) - \alpha(Y_1{}^2 + \cdots + Y_n{}^2)$ soit positive; pour $h \in V$, on aura alors:

$$(14) \qquad |{}_hf| \leqq \exp - \tfrac{1}{2}\alpha(x_1{}^2 + \cdots + x_n{}^2).$$

D'après la formule (12), la formule (14) et la forme de la mesure de Haar sur N, on a donc ${}_hf \in L^1{}_C(N, \rho)$ pour $h \in V$; de plus, pour h' fixé dans N, ${}_hf(h') = f(hh')$ dépend holomorphiquement de $h \in V$. L'inégalité (14) et le lemme 1 montrent que l'application $h \to {}_hf$ de V dans $L^1{}_C(N, \rho)$ est holomorphe, de sorte que f est un vecteur analytique de $L^1{}_C(N, \rho)$ pour la représentation régulière (lemme 2).

C) Soit $\mathscr{F}$ l'ensemble des fonctions sur N de la forme $\exp - F(y_1, \cdots, y_m)$ axec $F \in \mathfrak{Q}^+$ et soit $\mathscr{G}$ l'ensemble des combinaisons linéaires complexes d'éléments de $\mathscr{F}$. Pour démontrer le lemme, il reste à faire voir que $\mathscr{G}$ est partout dense dans $L^1{}_C(N, \rho)$, ce que nous ferons par une méthode un peu différente de celle de [1], pp. 218-220. Observons pour cela que la famille $\mathscr{F}$ a les propriétés suivantes:

1) Les fonctions de $\mathscr{F}$ sont continues, partout > 0 sur N, et nulles à l'infini d'après (14).

2) Le produit de deux fonctions de $\mathscr{F}$ est dans $\mathscr{F}$.

3) La famille $\mathscr{F}$ est invariante par les translations à gauche, car si $f = \exp - F(y_1, \cdots, y_m)$, on a ${}_hf = \exp - (\pi(h)F)(y_1, \cdots, y_m)$; mais pour $h \in N$, la matrice $\| a_{jk}(h) \|$ est réelle et par suite $\pi(h)F \in \mathfrak{Q}^+$ si $F \in \mathfrak{Q}^+$.

4) $\mathscr{F}$ sépare les points de N: raisonnant par l'absurde, supposons qu'il existe $h_0, h_1 \in N$ avec $h_1 \neq e$ et $f(h_0h_1) = f(h_0)$ pour toute $f \in \mathscr{F}$; d'après la propriété précédente, on aurait pour $f \in \mathscr{F}$ et $h \in N$:

$$f(hh_1) = {}_{hh_0^{-1}}f(h_0h_1) = {}_{hh_0^{-1}}f(h_0) = f(h)$$

d'où $f(h) = f(hh_1{}^m)$ pour toute $f \in \mathscr{F}$ et tout entier m. Mais lorsque m tend vers l'infini, il en est de même de $h_1{}^{m}$[4]; comme f est nulle à l'infini sur N, on en déduit $f = 0$, ce qui est absurde.

Alors, $\mathscr{G}$ est une algèbre de fonctions continues complexes sur N nulles à l'infini, séparant les points et stable par conjugaison. D'après le théorème de Stone-Weierstrass, toute fonction complexe continue nulle à l'infini sur N est limite uniforme de fonctions de $\mathscr{G}$; soit alors f une fonction continue à support compact sur N; pour toute $f_0 \in \mathscr{F}$ et tout $\epsilon > 0$, il existe $f_1 \in \mathscr{G}$ telle que $|ff_0{}^{-1} - f_1| \leqq \epsilon$, d'où $\int_N |f - f_0 f_1| \rho\, dh \leqq \epsilon \int_N \rho f_0\, dh$. Comme $f_0 f_1$ appartient à $\mathscr{G}$, on a montré que $\mathscr{G}$ est partout dense dans $L^1{}_C(N, \rho)$.

5. Un lemme de transition. Nous considérerons dans ce paragraphe la situation suivante:

G est un groupe de Lie connexe, K et N deux sous-groupes analytiques de G tels que $G = K \cdot N$; enfin Z est un sous-groupe central de G contenu dans K tel que $K^* = K/Z$ soit compact.

π est une représentation continue de G dans un espace de Banach $\mathfrak{H}$

μ est une représentation continue de K dans $\mathfrak{H}$ telle que:

a) quels que soient $s \in K$ et $s' \in G$, on a $\mu(s)\pi(s') = \pi(s')\mu(s)$;

b) l'application μ de K dans $\mathscr{L}(\mathfrak{H})$ est analytique (au sens de la norme de $\mathscr{L}(\mathfrak{H})$) ;

c) les restrictions de π et μ à Z sont identiques.

Soit $u \rightarrow u^*$ l'application canonique de K sur K^*; d'après c), l'opérateur $\mu(s)^{-1}\pi(s)$ est égal à 1 pour $s \in Z$, donc il existe une représentation continue π^* de K^* dans $\mathfrak{H}$ telle que $\mu(s)^{-1}\pi(s) = \pi^*(s^*)$ pour $s \in K$.

Ceci étant posé, on a le lemme suivant:

LEMME 7. *Soit f une fonction analytique sur K^* et soit ψ un élément de $\mathfrak{H}$, vecteur analytique de $\mathfrak{H}$ pour la représentation de N induite par π. Le vecteur $\phi = \int_{K^*} f(u^*)\pi^*(u^*)\psi\, du^*$ est un vecteur analytique de $\mathfrak{H}$ pour la représentation π.*

Nous pouvons étendre sans difficulté les raisonnements de [1], pp. 221-

---

[4] Si $h \in N$ est différente de e, h^m tend vers l'infini pour $m \rightarrow \infty$: sinon, d'après [4], chap. VI, lemme 2, les h^m seraient contenus dans un sous-groupe compact de G non réduit à e; mais si $x_i(h) \neq 0$ et $x_{i+1}(h) = \cdots = x_n(h) = 0$, la construction récurrente de H montre que l'on a $x_i(h^m) = m x_i(h)$, ce qui ne reste pas borné pour $m \rightarrow \infty$.

224. Pour $x \in G$, on a:

$$\pi(x)\phi = \int_{K^*} f(u^*)\pi(x)\pi^*(u^*)\psi \, du^*.$$

Posons, pour $x \in G$ et $u \in K$, $xu = u_x s(x,u)$ où $u_x \in K$ et $s(x,u) \in N$. Si $v \in Z$, on a $x(uv) = u_x s(x,u)v = (u_x v)s(x,u)$ puisque v est dans le centre de G. Donc $(u_x)^*$, $s(x,u)$ et $u^{-1}u_x$ ne dépendent que de x et de u^*. Nous noterons ces éléments u_x^*, $s(x,u^*)$ et $\gamma(x,u^*)$. Les applications $(x,u^*) \rightarrow u_x^*$, $(x,u^*) \rightarrow s(x,u^*)$ et $(x,u^*) \rightarrow \gamma(x,u^*)$ sont analytiques et l'on a:

$$\begin{aligned}\pi(x)\pi^*(u^*) &= \pi(x)\mu(u)^{-1}\pi(u) = \mu(u)^{-1}\pi(u_x)\pi(s(x,u)) \\ &= \mu(u)^{-1}\mu(u_x)\pi^*(u_x^*)\pi(s(x,u^*)) = \mu(\gamma(x,u^*))\pi^*(u_x^*)\pi(s(x,u^*)).\end{aligned}$$

Donc: $\pi(x)\phi = \int_{K^*} f(u^*)\mu(\gamma(x,u^*))\pi^*(u_x^*)\pi(s(x,u^*))\psi \, du^*.$

Pour x fixé, les applications $u \rightarrow u_x$ et $u \rightarrow u_{x^{-1}}$ sont des applications analytiques réciproques l'une de l'autre de K dans K. Donc les applications $u^* \rightarrow u_x^*$ et $u^* \rightarrow u_{x^{-1}}^*$ sont des automorphismes réciproques de la variété analytique K^*. Posons $du_x^* = D(x,u^*)du^*$, où D est une fonction analytique sur $G \times K^*$. On a:

$$\pi(x)\phi = \int_{K^*} \pi^*(u^*)D(x^{-1},u^*)f(u_{x^{-1}}^*)\mu(\gamma(x,u_{x^{-1}}^*))\pi(s(x,u_{x^{-1}}^*))\psi \, du^*.$$

Posons: $\psi(x,u^*) = D(x^{-1},u^*)f(u_{x^{-1}}^*)\mu(\gamma(x,u_{x^{-1}}^*))\pi(s(x,u_{x^{-1}}))\psi$. D'après le choix de ψ, $\pi(s(x,u_{x^{-1}}^*))\psi$ dépend analytiquement de (x,u^*); l'application $(\alpha,\beta,T,\eta) \rightarrow \alpha\beta(T\cdot\eta)$ de $\boldsymbol{R} \times \boldsymbol{R} \times \mathfrak{L}(\mathfrak{H}) \times \mathfrak{H}$ dans $\mathfrak{H}$ est multilinéaire et continue et $(x,u^*) \rightarrow \mu(\gamma(x,u_{x^{-1}}^*))$ est une application analytique de $G \times K^*$ dans $\mathfrak{L}(\mathfrak{H})$. Il en résulte que $\psi(x,u^*)$ dépend analytiquement de $(x,u^*) \in G \times K^*$; comme K^* est compact, il existe d'après le lemme 4 un voisinage V de e dans G et un système de coordonnées analytiques $(t_1,\cdots,t_n)$ dans V tels que, pour $(x,u^*) \in V \times K^*$, on ait:

$$\psi(x,u^*) = \sum_{e} \psi_e(u^*)t_1^{e_1}(x)\cdots t_n^{e_n}(x), \qquad \boldsymbol{e} = (e_1,\cdots,e_n) \in \boldsymbol{N}^n$$

où les applications ψ_e de K^* dans $\mathfrak{H}$ sont continues; la somme précédente converge uniformément et absolument dans $V \times K^*$. Alors:

$$\begin{aligned}\pi(x)\phi &= \int_{K^*} \pi^*(u^*)\psi(x,u^*)\,du^* \\ &= \sum_{e}\left\{\int_{K^*} \pi^*(u^*)\psi_e(u^*)\,du^*\right\} t_1^{e_1}(x)\cdots t_n^{e_n}(x)\end{aligned}$$

cette dernière famille de vecteurs étant encore sommable. Donc $x \rightarrow \pi(x)\phi$ est analytique dans V, ce qui, avec le lemme 2, achève la démonstration.

6. Vecteurs analytiques. Cas général. Nous commencerons par démontrer un lemme concernant la structure des groupes de Lie réels généraux. Ce lemme est contenu dans les résultats d'Iwasawa [3].

LEMME 8. *Soit G un groupe de Lie réel connexe et simplement connexe. Il existe des sous-groupes fermés K et N de G, et un sous-groupe discret Z du centre de G, avec les propriétés suivantes:*

(i) $$G = K \cdot N;$$

(ii) *N est résoluble connexe et simplement connexe;*

(iii) *K est produit direct d'un groupe compact K' et d'un groupe abélien connexe et simplement connexe A;*

(iv) *$Z \subset A$ et A/Z est compact.*

Comme G est simplement connexe, il est produit semi-direct d'un groupe de Lie semi-simple connexe et simplement connexe S et d'un groupe de Lie résoluble connexe et simplement connexe R (utiliser une décomposition de Levi de l'algèbre de Lie de G et construire *a priori* un tel produit semi-direct, qui sera isomorphe à G, puisque deux groupes de Lie connexes et simplement connexes ayant des algèbres de Lie isomorphes sont isomorphes). Les groupes S et R sont des sous-groupes fermés de G, et R est le radical de G. L'application $(s, r) \to sr$ est un isomorphisme de la variété analytique $S \times R$ sur la variété analytique G.

Il existe d'autre part (cf. par exemple [1], p. 223) des sous-groupes fermés K et M de S et un sous-groupe discret Z^0 du centre de S, possédant les propriétés suivantes:

a) $$S = K \cdot M;$$

b) M est résoluble connexe et simplement connexe;

c) K est produit direct d'un groupe compact K' et d'un groupe abélien connexe et simplement connexe A contenant Z^0, avec A/Z^0 compact.

Soit Z' l'intersection des noyaux des représentations linéaires continues de dimension finie de S. On sait que Z' est contenu dans le centre de S, et que S/Z' a un centre fini, de sorte que Z' est d'indice fini dans le centre de S. Donc $Z = Z' \cap Z^0$ est d'indice fini dans Z^0 et par suite A/Z est compact. Soit ρ la représentation adjointe de G dans l'algèbre de Lie $\mathfrak{g}$ de G; sa restriction à S est une représentation linéaire continue de dimension finie de S; son noyau contient donc Z' et par suite, pour $s \in Z$, on a $\mathrm{Ad}_{\mathfrak{g}}\, s = 1$; donc Z est contenu dans le centre de G.

Soit $N = M \cdot R$; comme R est distingué dans G, N est un sous-groupe fermé de G. En outre N/R est isomorphe à M, donc résoluble, de sorte que N est résoluble; comme M et R sont simplement connexes et que $N = M \cdot R$, N est simplement connexe. Enfin, comme $G = S \cdot R$ et que $S = K \cdot M$, on a $G = K \cdot N$.—c. q. f. d.

Nous allons maintenant démontrer le résultat central de cet article.

THÉORÈME. *Soient G un groupe de Lie réel, $\mathfrak{H}$ un espace de Banach et π une représentation continue de G dans $\mathfrak{H}$. Les vecteurs de $\mathfrak{H}$ analytiques pour π sont partout denses dans chacun des trois cas suivants:*

1) *G est connexe et simplement connexe; si Z désigne le sous-groupe introduit dans le lemme 8, les opérateurs $\pi(z)$ pour $z \in Z$ sont scalaires.*

2) *G est connexe et simplement connexe, et l'ensemble des opérateurs $\pi(z)$ pour $z \in Z$, est borné dans $\mathscr{L}(\mathfrak{H})$.*

3) *La représentation π est bornée, c'est-à-dire que l'ensemble des opérateurs $\pi(s)$ pour $s \in G$, est borné dans $\mathscr{L}(\mathfrak{H})$.*

Lorsque G est *résoluble* connexe et simplement connexe, les vecteurs analytiques sont partout denses dans $\mathfrak{H}$, comme il résulte des lemmes 3 et 6.

Supposons G connexe et simplement connexe et introduisons les groupes K, A, N et Z du lemme 8; comme A est abélien connexe et simplement connexe, il est produit direct de deux sous-groupes A' et A'', Z étant contenu dans A'' et image de $\mathbf{Z}^p$ par un isomorphisme ϕ de $\mathbf{R}^p$ sur A'' ($p = \dim A''$).

Dans le cas 1), posons $\pi(z) = \chi(z) \cdot 1$ pour $z \in Z$; il est clair que l'homomorphisme χ de Z dans le groupe multiplicatif $\mathbf{C}^*$ des nombres complexes se prolonge en un homomorphisme continu χ' de A'' dans $\mathbf{C}^*$. Comme K est produit direct de K', A' et A'', on peut prolonger χ' en un homomorphisme χ'' de K dans $\mathbf{C}^*$ égal à 1 sur K' et A'; on posera $\mu(u) = \chi''(u) \cdot 1$ et l'homomorphisme μ de K dans le groupe des opérateurs continus inversibles de $\mathfrak{H}$, est une application analytique de K dans $\mathscr{L}(\mathfrak{H})$.

Dans le cas 2), l'expression $\rho(s) = \sup \| \pi(sz) \|$, $z \in Z$, est finie pour tout $s \in G$ et représente une semi-norme sur G telle que $\rho(sz) = \rho(s)$ pour $z \in Z$ et $s \in G$; introduisons la représentation régulière π' de G dans $L^2{}_C(G, \rho)$. Comme ρ est invariante par les translations par les éléments de Z, les opérateurs $\pi'(z)$ sont unitaires pour $z \in Z$; posons:

$$\pi'(\phi(e_1, \cdots, e_p)) = U_1{}^{e_1} \cdots U_p{}^{e_p} \qquad (e_1, \cdots, e_p \in \mathbf{Z})$$

où les U_i sont unitaires. On peut écrire $U_i = \exp H_i \sqrt{-1}$, où l'opérateur hermitien continu H_i commute à tout opérateur commutant à U_i; soit alors

μ la représentation de A'' dans $\mathfrak{H}$ definie par:

$$\mu(\phi(t_1,\cdots,t_p)) = \prod_{i=1}^{p} \exp \sqrt{-1}\, t_i H_i \qquad (t_1,\cdots,t_p \in \mathbf{R})$$

que nous prolongerons à K en posant $\mu(k'a'a'') = \mu(a'')$ pour $k' \in K'$, $a' \in A'$ et $a'' \in A''$. L'application μ de K dans $\mathfrak{L}(L^2{}_C(G,\rho))$ est alors analytique et les opérateurs $\mu(u)$ commutent à tout opérateur commutant aux U_i, en particulier ils commutent aux $\pi'(s)$ $(s \in G)$. On a enfin $\mu(u) = \pi(u)$ pour $u \in Z$.

On notera alors, que pour tout groupe compact, les fonctions analytiques sont partout denses dans l'espace des fonctions intégrables pour la mesure de Haar, puisqu'il en est ainsi des coefficients des représentations continues de dimension finie. Le lemme 7 et ce qu'on a vu des groupes résolubles montrent alors que, dans le cas 1) les vecteurs analytiques sont partout denses dans $\mathfrak{H}$, et dans le cas 2) les vecteurs analytiques pour la représentation π' sont partout denses dans $L^2{}_C(G,\rho)$. D'autre part, l'application $(f,g) \rightarrow fg$ est une application bilinéaire continue de $L^2{}_C(G,\rho) \times L^2{}_C(G,\rho)$ dans $L^1{}_C(G,\rho)$; donc les vecteurs de $L^1{}_C(G,\rho)$ analytiques pour la représentation régulière sont partout denses dans $L^1{}_C(G,\rho)$. D'après le lemme 3, les vecteurs analytiques pour la représentation π sont donc partout denses dans $\mathfrak{H}$, dans le cas 2).

Dans le cas 3), soit G_0 la composante connexe de e dans G et soit $G_0{}^*$ le revêtement universel de G_0; la représentation π de G définit de manière bien déterminée une représentation continue bornée π^* de $G_0{}^*$. D'après 2), les vecteurs de $\mathfrak{H}$ analytiques pour π^* sont partout denses dans $\mathfrak{H}$; mais comme $G_0{}^*$ est localement isomorphe à G_0, un vecteur de $\mathfrak{H}$ analytique pour π^* est analytique pour la restriction de π à G_0 et donc pour π (lemme 2).—c.q, f. d.

Appendice.

LEMME A. *Soit* $U = \| u_{ij} \|$ *une matrice à coefficients complexes, à* n *lignes et* n *colonnes; on suppose* $u_{ij} = 0$ *pour* $i < j$*; on considère les* $u_{ii} = a_i$ *comme des constantes et l'on note* t *une variable complexe. Dans ces conditions, les coefficients de la matrice* $\exp tU$ *sont de la forme*

$$\sum_{\alpha} E_\alpha(t) P_\alpha(u_{21}, u_{31}, \cdots, u_{n,n-1})$$

où les P_α *sont des polynomes de degré* $< n$ *et les* E_α *sont tous de la forme*

$$\sum_{i=1}^{n} e^{a_i t} Q_i(t), \tag{15}$$

Q_i *étant un polynome de degré* $< n$.

Soit $V(t) = \exp tU$. On sait que $dV(t)/dt = U \cdot V(t)$, d'où

$$\prod_{i=1}^{n} (d/dt - a_i) V(t) = \prod_{i=1}^{n} (U - a_i \cdot 1) \cdot V(t) = 0$$

puisque, d'après le théorème de Hamilton-Cayley, on a $\prod_{i=1}^{n} (U - a_i \cdot 1) = 0$. Les coefficients de $V(t)$ sont donc, lorsque les u_{ij} $(i > j)$ sont fixés, solutions de l'équation differentielle $\prod_{i=1}^{n} (d/dt - a_i) f(t) = 0$, donc de la forme (15).

Considérons maintenant t comme fixé. On peut décomposer de manière unique U en somme d'une matrice diagonale D et d'une matrice N avec $n_{ij} = 0$ pour $i \leqq j$ (et donc $n_{ij} = u_{ij}$ pour $i > j$). Soit (e_i) la base canonique de $\boldsymbol{C}^n$, et considérons D et N comme des endomorphismes de $\boldsymbol{C}^n$; si V_i est le sous-espace de $\boldsymbol{C}^n$ de base $(e_i, e_{i+1}, \cdots, e_n)$, on a $D(V_i) \subset V_i$ et $N(V_i) \subset V_{i+1}$, il en résulte que tout monôme (non commutatif) en D et N dont le degré en N est $\geqq n$ est nul; par suite, pour tout entier m, les coefficients de $(D + N)^m$ sont, pour D fixé, des polynomes de degré $< n$ en les u_{ij} $(i > j)$; il en résulte que, pour t et D fixés, les coefficients de $\exp t(D + N) = \sum_{m \geqq 0} t^m (D + N)^m / m!$ sont des polynomes de degré $< n$ en les u_{ij} $(i > j)$:

Ceci posé, le lemme A est une conséquence du lemme facile suivant, dont on laisse la démonstration au lecteur:

LEMME B. *Soient X et Y deux ensembles, K un corps, V (resp. W) un espace vectoriel de dimension finie de fonctions sur X (resp. Y). Soit f une application de $X \times Y$ dans K telle que:*

a) *pour tout $x \in X$, l'application $y \to f(x, y)$ est dans W;*

b) *pour tout $y \in Y$, l'application $x \to f(x, y)$ est dans V.*

Alors f est de la forme $f(x, y) = \sum_{\alpha} g_\alpha(x) h_\alpha(y)$ avec $g_\alpha \in V$ et $h_\alpha \in W$.

UNIVERSITY OF PARIS.

BIBLIOGRAPHIE.

[1] Harish-Chandra, "Representations of a semi-simple Lie group on a Banach space I," *Transactions of the American Mathematical Society*, vol. 75 (1953), pp. 185-243.

[2] E. Hille, *Functional analysis and semi-groups*, American Mathematical Society Colloquium Publications, vol. 31, New York, 1948.

[3] Iwasawa, "On some types of topological groups," *Annals of Mathematics*, vol. 50 (1949), pp. 507-558.

[4] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, 2ème édition, *Actualités Scientifiques et Industrielles*, no. 1154, Paris, Hermann.

THE PROBLEM OF MINIMAL MODELS IN THE THEORY OF ALGEBRAIC SURFACES.*

By Oscar Zariski.†

Introduction. The non-singular varieties, in a given birational class of varieties (over an algebraically closed field k), form—in a well-known fashion—a partially ordered set $\mathfrak{B}$. Any minimal element of $\mathfrak{B}$ is called a *relatively minimal model*, and the lower bound of $\mathfrak{B}$ (if it exists) is called a *minimal model* (we identify biregularly equivalent varieties). The object of the present paper is to prove, for ground fields of arbitrary characteristic, the following classical result (known to the Italian geometers in the classical case):[1] *if a birational class $\mathfrak{B}$ of non-singular surfaces contains no minimal model then $\mathfrak{B}$ is the birational class of a ruled surface* (§ 3, Fundamental Theorem A). We prove actually a stronger result. It can be proved that if our birational class of non-singular surfaces contains no minimal model and if F is a relatively minimal model in the class (such models always exist even in the case of higher varieties, as long as our birational class contains non-singular models at all; see Corollary 1.8), then F carries an irreducible exceptional curve E of the second kind (Proposition 3.3, (a) and Proposition 2.6). It can also be shown that the self-intersection number (E^2) of an irreducible exceptional curve E of the second kind (on a non-singular surface F) is $\geqq 0$ (and that if E has singularities then $(E^2) > 0$); see Proposition 2.7. Then

---

* Received October 24, 1957.

† This research was supported by the United States Air Force through the Air Office of Scientific Research of the Air Research and Development Command under Contract No. AF18(600)-1503.

[1] See, for instance, F. Enriques [2], pp. 372-374. The proof in the classical case is due to Castelnuovo and Enriques, but that proof cannot be regarded as entirely rigorous. Furthermore, some steps of the proof, even those which could be accepted without objections in the classical case, would break down in the case of characteristic $p \neq 0$. Our proof differs from the classical proof also in some of its central ideas. Thus: (a) we do not have to presuppose that the Castelnuovo criterion of rationality $p_a = P_2 = 0$ has already been established (and in fact, the validity of that criterion does not result from our proof, except in some special cases; see, however, the concluding remarks of our introduction); (b) the crucial phases of the proof are based on specific properties of exceptional curves of the second kind.

what we actually prove is the following stronger result: *if a non-singular surface F carries an irreducible exceptional curve E of the second kind, then F is birationally equivalent to a ruled surface, and that if, furthermore, (E^2) is positive then F is a rational surface* (Fundamental Theorem B, § 3).

A preliminary study of the problem of minimal models is contained in our monograph "Introduction to the problem of minimal models in the theory of algebraic surfaces," now in course of publication in the "Publications of the Mathematical Society of Japan." In that monograph (based on a series of lectures given in Tokyo and Kyoto in the fall of 1956) we give an exposition of some background material concerning rational transformations and linear systems, then develop the theory of exceptional curves on a non-singular surface, and finally give an outline of the contents of the present paper. This monograph will be referred to as IP. Frequent and explicit references to various propositions proved in IP will be made in the present paper, especially in regard to the theory of exceptional curves.

In Section 1 we deal with varieties of any dimension and we prove that the class $\mathfrak{B}$ satisfies the descending chain condition (Proposition 1.5). Thus the existence of relatively minimal models as assured (as long as $\mathfrak{B}$ is non-empty; a question which is still open for varieties of dimension > 2 in the case of characteristic $\neq 0$, and for varieties of dimension > 3 in the case of characteristic zero). This result is a rather straightforward consequence of the theorem of Neron-Severi.[2] In Section 2 we review some of the results concerning exceptional curves which have been obtained in IP, and we derive a few other properties of exceptional curves. In Section 3 we give various criteria of existence of minimal models. In partilular, we show that if there does *not* exist a minimal model then we are dealing with surfaces all plurigenera of which are zero' (Proposition 2.9). This result (above all, the vanishing of the geometric genus p_g and of the bigenus P_2) is repeatedly used in the rest of the paper. In Section 4 we prove the fundamental theorem B (stated in Section 3) under the assumption that $(E^2) = 0$ and also in the case in which E is non-singular. The conditions $p(E) = 0$ and $(E^2) \geqq 0$ characterize the irreducible *non-singular* exceptional curves of the second kind (Proposition 2.8), and what we are actually proving in Section 4 is that if a non-singular surface F carries an irreducible curve E such that $p(E) = 0$ and $(E^2) \geqq 0$, then F is birationally equivalent to a ruled surface.

---

[2] In the case of surfaces it is possible (as was pointed out by Serre) to prove the descending chain condition by using sheaf theory. Namely, one observes that if $F < F'$, where F and F' are non-singular surfaces, then $h^{1,1}(F) < h^{1,1}(F')$, where the notations are those of the theory of sheaves. This inequality is first proved directly in the case in which the birational transformation $F \rightarrow F'$ is locally quadratic, and then one uses our factorization theorem for antiregular birational transformations of non-singular surfaces (see IP, Theorem II. 1. 2; or also our paper [12], Lemma on p. 538).

A second proof (which we shall publish in the Mem. Col. Sci. of Kyoto University) is based on the consideration of the anticanonical system $|-K|$ of an algebraic surface. It can be shown that if we have an infinite strictly descending chain $F_1 > F_2 > \cdots$ of non-singular algebraic surfaces, then $\dim |-K(F_j)| \rightarrow +\infty$, and this can be shown to lead to a contradiction.

The remainder of the paper deals with the proof of the fundamental theorem B in the case $(E^2) > 0$. In this case it is the rationality of F that has to be proved. A first step in that direction is the proof of the vanishing of the arithmetic genus p_a of F (Section 5). It will be noted that our present proof of the vanishing of p_a is much simpler than the proof which was outlined in IP (III, § 3). We now make no use of the concept of strongly minimal models (IP, Definition III. 3. 1), and—what is more important—we do not use a local result which was stated without proof in IP (Proposition III. 3. 4). The proof of this local result will be published elsewhere. What is common to both proofs is the recourse to Abelian varieties and the use of the equality $q = -p_a$, which holds on any surface of geometric genus zero.

The proof of the fundamental theorem in the case $(E^2) > 0$ (and under the permissible assumption that F is a relatively minimal model; see remark at the end of Section 5) has to be divided into various cases, according to the value of (K^2), where K is a canonical divisor on F. A very short proof, given in Section 6, settles the case $(K^2) \leqq 0$. In Section 7 we develop some general properties of surfaces which satisfy the Castelnuovo criterion $p_a = P_2 = 0$ *and* the inequality $(K^2) > 0$. In Section 8 we prove the Castelnuovo criterion of rationality in the case $(K^2) \geqq 3$. This leaves us only with two cases for completing the proof of the fundamental theorem: $(K_2) = 1$ and $(K^2) = 2$. The proof in the case $(K^2) = 1$ (Section 9) is very short and simple. In the last section (Section 10) we deal with the case $(K^2) = 2$, and here again, as in Section 8, we are proving not merely the fundamental theorem B but actually the Castelnuovo criterion of rationality $p_a = P_2 = 0$ in the case $(K^2) = 2$ (the latter implies the former once the vanishing of p_a has been established in Section 5). We first give a very simple proof, but unfortunately this proof does not work for characteristic 2. We then give a second (and much longer) proof which is valid for any characteristic. This second proof is constructive in the sense that we construct the entire family of algebraic surfaces with $p_a = P_2 = 0$ and $(K^2) = 2$. We show that the general member of this family is a rational surface, and we then prove the rationality of the given surface F by a specialization argument.

From the foregoing outline it is seen that the present investigation contains a proof of Castelnuovo's criterion of rationality of a surface ("a surface is rational if $p_a = P_2 = 0$") in the case $(K^2) \geqq 2$. A proof of Castelnuovo's criterion of rationality, in the classical case, was given by Kodaira in a lecture course at Princeton in 1956 (the existence of this proof, and the proof itself, because known to me in Paris through an exposé by Serre in a Bourbaki seminar in 1957). It appears clearly from that exposé that Kodaira's proof, *in the case* $(K^2) \leqq 0$, is algebraic in nature and is valid for any characteristic. [On the contrary, in the case $0 < (K^2) \leqq 9$, Kodaira's proof uses topological considerations; our proof in the case $(K^2) \geqq 3$ was presented in a Kyoto seminar in 1956 and is similar to, but somewhat simpler than, the proof of Kodaira in the case $(K^2) > 9$]. Thus the proof of Castelnuovo's criterion of rationality in the abstract case is complete, except for the case $(K^2) = 1$. We have a proof also in this case, but in order not to lengthen the present paper we do not include it here; it will be published elsewhere.

We point out that the proof of the fundamental theorem in the case $(K^2) \leqq 0$ which we gave in our Kyoto seminar was very long, while in the present paper the proof takes a few lines (Section 6). The reason for this is that in the Kyoto seminar we were essentially proving also the Castelnuovo criterion of rationality in the case $(K^2) \leqq 0$ (and not merely the fundamental theorem B). However, our Kyoto proof of Castelnuovo's criterion of rationality in the case $(K^2) \leqq 0$ was not as simple as Kodaira's proof and is therefore superseded by the latter.

TABLE OF CONTENTS.

1. Minimal and relatively minimal models.
2. Exceptional curves of the 1st and 2nd kind.
3. Preliminary criteria of existence of minimum models and statement of the main results.
4. The case $(E^2) = 0$.
5. Case $(E^2) > 0$. The vanishing of $p_a(F)$.
6. The case $(E^2) > 0$, $(K^2) \leqq 0$.
7. Some general properties of surfaces with $p_a = P_2 = 0$ and $(K^2) > 0$.
8. Proof of Castelnuovo's criterion of rationality in the case $(K^2) \geqq 3$.
9. Proof of the fundamental theorem B in the case $(K^2) = 1$.
10. Proof of Castelnuovo's criterion of rationality in the case $(K^2) = 2$.

1. Minimal and relatively minimal models. Let k be an algebraically closed field and let Σ be a field of algebraic functions of r independent variables over k, i.e., a finitely generated extension of k, of transcendence degree r. By a *projective model* of Σ/k we mean a pair (V, P), where V is a (projective) variety which is defined and irreducible over k, P is a general point of V/k, and $\Sigma = k(P)$. In the sequel we shall often refer to V itself as a projective model of Σ/k and shall write V instead of (V, P) without fear of confusion.

We shall denote by $\mathfrak{B}^*$ the totality of all normal projective models of Σ/k, and by $\mathfrak{B}$ the totality of all non-singular projective models of Σ/k.

Given two projective models $V = (V, P)$ and $V' = (V', P')$ of Σ/k, there is a unique birational transformation T of V onto V' such that $T(P) = P'$. We shall say that V *dominates* V', or in symbols: $V \succ V'$, if T is regular on V. The relation $\succ$ defines a partial ordering of the birational class $\mathfrak{B}^*$. As a rule we shall identify biregularly equivalent models, i.e., models V and V' such that $V \succ V'$ *and* $V' \succ V$.

Let V, V' be members of $\mathfrak{B}^*$ such that $V \succ V'$ and let $T\colon V \rightarrow V'$ be the regular transformation of V onto V'. To any irreducible subvariety W/k of V/k there corresponds a unique irreducible subvariety W'/k of V'/k, and we have $\dim W' \leqq \dim W$. We say that W is an exceptional variety of T if $\dim W' < \dim W$. It is known (see IP, Corollary I. 2. 4) that there exists a subvariety E of V, called the *exceptional locus* of T, having the following properties: 1) E is defined over k; 2) every irreducible component of E/k is an exceptional variety of T; 3) every exceptional variety of T is contained in E. The exceptional locus E of T is identional with the set of all points of V at which T is not biregular.

Let $\mathfrak{G}$ denote the group of divisorial cycles on V which is generated by the prime divisorial cycles which are rational over k. Let $\mathfrak{G}'$ have the similar meaning for the variety V'. We shall now associate with the regular transformation $T\colon V \rightarrow V'$ a mapping, denoted by the same letter T, of $\mathfrak{G}$ into $\mathfrak{G}'$.

If Z is a prime divisorial cycle on V, rational over k, and if the variety Z is not exceptional for T, then the corresponding variety on V' is of the same dimension as Z and defines a prime divisorial cycle Z', rational over k. We then set $T(Z) = Z'$. If, however, Z is an exceptional variety we set $T(Z) = 0$. We then extend the definition of the cycle transformation $Z \rightarrow T(Z)$ to the whole group $\mathfrak{G}$, by linearity. If we denote by $\mathfrak{G}(T)$ the subgroup of $\mathfrak{G}$ generated by prime divisorial cycles which are exceptional for T, then the cycle transformation T is a homomorphism of $\mathfrak{G}$ into $\mathfrak{G}'$, with kernel $\mathfrak{G}(T)$. It is clear that T is a mapping of $\mathfrak{G}$ onto $\mathfrak{G}'$, for every $(r-1)$-dimensional irreducible subvariety W'/k of V'/k corresponds, under T, to at least one irreducible subvariety W/k of V/k.

Let $\mathfrak{G}_a$ (resp. $\mathfrak{G}'_a$) be the subgroup of $\mathfrak{G}$ (resp. of $\mathfrak{G}'$) which is generated by the cycles which are algebraically equivalent to zero.

PROPOSITION 1.1. *Denoting by* $\mathfrak{E}(T)+\mathfrak{G}_a$ *the subgroup of* $\mathfrak{G}$ *which is generated by the subgroups* $\mathfrak{E}(T)$ *and* $\mathfrak{G}_a$, *we have*

$$T(\mathfrak{E}(T)+\mathfrak{G}_a)=\mathfrak{G}'_a.$$

Proof. We shall use notations and results from Weil's paper [10]. Any cycle in $\mathfrak{G}_a$ is of the form $Z(N)-Z(M)$, where Z is a divisorial cycle on the product $V\times C$ of V by a non-singular irreducible curve C/k and where M and N are points of C which are rational over k (Weil [10], Lemma 10). Here the divisorial cycle Z may be assumed to be a "reduced" one, i.e., free from prime components of the form $V\times W'$ or $W\times C$ ($W'\in V'$, $W\subset V$). As to the symbol $Z(Q)$, where Q is a point of C, it is defined by the relation $Z(Q)\times Q=Z\cdot V\times Q$. Since Z is a reduced divisorial cycle and both V and C are normal, it is true for any point Q of C that all the prime components of the cycle $Z\cdot V\times Q$ are proper intersections of the variety of the cycle Z with the variety $V\times Q$, i.e., they are all of dimension $r-1$ and are simple for $V\times C$ (and also for $V\times Q$). They are therefore all of the form $\Gamma\times Q$, where Γ is a prime divisorial cycle on V. Thus $Z(Q)$ is a divisorial cycle on V.

The birational transformation $T^*\colon V\times C\to V'\times C$ defined $T^*(A\times B)=T(A)\times B$ ($A\in V, B\in C$) is regular. By the preceding definition, we have an induced transformation, denoted by the same letter T^*, of the group of divisorial cycles of $V\times C$ onto the group of divisorial cycles of $V'\times C$. We set $Z'=T^*(Z)$. We now observe that if Q is a rational point of C, then the restriction to $V\times Q$ of the birational transformation $T^*\colon V\times C\to V'\times C$ is a birational transformation $T_Q\colon V\times Q\to V'\times Q$, defined over k, and it is immediate that for any divisorial cycle Γ on V we have

$$T_Q(\Gamma\times Q)=T(\Gamma)\times Q. \tag{1}$$

We have the following relation:

$$T^*(Z)\cdot V'\times Q=T_Q(Z(Q)\times Q). \tag{2}$$

In fact, let Γ be any prime divisorial cycle on V, rational over k. If Γ is not an exceptional variety of T, then T is biregular at a general point of Γ/k, T^* is biregular at a general point of $\Gamma\times Q/k$. In this case, the coefficient of $\Gamma\times Q$ in $Z\cdot V\times Q$ is the same as the coefficient of $T(\Gamma)\times Q$ in

$T^*(Z)\cdot V'\times Q$. On the other hand, the coefficient of $\Gamma\times Q$ in $Z\cdot V\times Q$ is the same as the coefficient of $T(\Gamma)\times Q$ in $T_Q(Z\cdot V\times Q)$, by the definition of the cycle transformation T_Q. Hence in this case, the cycle $T(\Gamma)\times Q$ occurs with the same coefficient in both sides of (2). Now, assume that Γ is an exceptional variety of T. In that case, $\Gamma\times Q$ is also an exceptional variety of T_Q [by (1)], and thus $T_Q(\Gamma\times Q)=0$. Since any prime divisorial cycle of $V'\times Q$ is the T_Q-transform of a cycle of the form $\Gamma\times Q$, where Γ is a non-exceptional prime divisor cycle of V, relation (2) is established.

We now go back to our cycle $Z(N)-Z(M)$ in $\mathfrak{G}_a$. Let $Z(M)=\sum a_i\Gamma_i$, $Z(N)=\sum b_j\Delta_j$, where Γ_i and Δ_j are prime divisorial cycles on V, rational over k. We have

$$Z\cdot V\times M=\sum a_i(\Gamma_i\times M),\qquad Z\cdot V\times N=\sum b_j(\Delta_j\times N).$$

Hence, by (2),

$$Z'\cdot V'\times M=\sum a_i(T(\Gamma_i)\times M),\qquad Z'\cdot V'\times N=\sum b_j(T(\Delta_j)\times N),$$

where $Z'=T^*(Z)$. Consequently

$$Z'(M)-Z'(N)=T(Z(M)-Z(N)). \tag{3}$$

This establishes the inclusion $T(\mathfrak{G}_a)\subset\mathfrak{G}'_a$ and therefore also the inclusion $T(\mathfrak{E}(T)+\mathfrak{G}_a)\subset\mathfrak{G}'_a$, since $\mathfrak{E}(T)$ is the kernel of T. The opposite inclusion $\mathfrak{G}'_a\subset T(\mathfrak{G}_a)$ follows from the fact that given any reduced divisorial cycle Z' on $V'\times C$ there exists a reduced divisorial cycle Z on $V\times C$ such that $Z'=T^*(Z)$. This completes the proof of the proposition.

COROLLARY 1.2. *The group of Neron-Severi of the variety V' (i. e., the group $\mathfrak{G}'/\mathfrak{G}'_a$) is isomorphic to $\mathfrak{G}/(\mathfrak{E}(T)+\mathfrak{G}_a)$ and is therefore a homomorphic image of the group of Neron-Severi of the variety V.*

COROLLARY 1.3. *If the exceptional locus E of T has dimensional $r-1$ then the number of Picard $\rho(V')$ of V' ($\rho(V')=$ rank of $\mathfrak{G}'/\mathfrak{G}'_a$) is less than the number of Picard $\rho(V)$ of V.*

For under our assumption, there exists a prime divisorial cycle Γ on V such that $T(\Gamma)=0$, and the corollary follows from the fact that no integral multiple $n\Gamma$ of Γ $(n\neq 0)$ can be algebraically equivalent to zero.

COROLLARY 1.4. *If V is either a non-singular variety or is a normal surface, and if the regular transformation $T\colon V\rightarrow V'$ is not biregular, then $\rho(V)>\rho(V')$.*

For in either case the exceptional locus E of T has dimension $r-1$

(van der Waerden, *Algebraische Korrespondenzen und rationale Abbildungen*, Math. Ann. *110*, 1934, p. 154; Zariski, *Foundations of a general theory of birational correspondences*, Trans. Amer. Math. Soc., *53*, 1943, p. 532, Corollary to Theorem 17).

As a consequence of Corollary 1.4 and the finiteness of the number ρ of Picard we have

PROPOSITION 1.5. *The birational class $\mathfrak{B}$ of non-singular projective models of Σ/k satisfies the descending chain condition. If $r = 2$ then also the birational class $\mathfrak{B}^*$ (of normal projective models of Σ/k) satisfies the descending chain condition.*

Note that in this proposition it is tacitly assumed that biregularly equivalent varieties have been identified.

DEFINITION 1.6. *By a relatively minimal model of Σ/k we mean a minimal element o fthe ordered set $\mathfrak{B}$, i. e., a non-singular projective model V of Σ/k which does not dominate (in the strict sense) any other non-singular projective model of Σ/k.*

DEFINITION 1.7. *By a minimal model of Σ/k we mean a lower bound of the ordered set $\mathfrak{B}$, i. e., a non-singular projective model V of Σ/k such that $V \prec V'$ for all non-singular projective models V' of Σ/k.*

COROLLARY 1.8. *If a field Σ/k of algebraic functions of r independent variables possesses at all non-singular projective models (in particular, if $r = 2$, or if $r = 3$ and the characteristic of k is 0) then Σ/k also possesses a relatively minimal model, and, in fact, given any non-singular projective model V of Σ/k there exists a relatively minimal model V' of Σ/k such that $V' \prec V$.*

This follows from the descending chain condition in $\mathfrak{B}$ (Proposition 1.5).

If there exists a minimal model of Σ/k, then there is only one such model. On the other hand, it follows from Corollary 1.8 that if there does not exist a minimal model of Σ/k and if the class $\mathfrak{B}$ is not empty, then there exist at least two distinct relatively minimal models of Σ/k (distinct = not biregularly equivalent).

2. Exceptional curves of the 1st and 2nd kind. The problem of minimal models for algebraic surfaces requires a preliminary study of exceptional curves on an algebraic surface. This preliminary work has been carried out in Part II of our paper IP and will be briefly reviewed here (without proofs).

DEFINITION 2.1. *An algebraic curve E (reducible or not) on a normal surface F is said to be an exceptional curve of F if there exists a birational transformation $T: F \rightarrow F'$ of F onto a surface F' such that E is the* TOTAL *T^{-1}-transform of a* SIMPLE *point of F'.*

DEFINITION 2.2. *An exceptional curve E of a normal surface F is said to be* OF THE FIRST KIND *if there exists a birational transformation T satisfying the condition stated in the preceding definition and satisfying the further condition that it be regular at each point of E. In the contrary case E is said to be an exceptional curve* OF THE SECOND KIND.

Given a curve E (on F) and a birational transformation $T: F \rightarrow F'$ such that E is the total T^{-1}-transform of a *normal* point P' of F', we shall say, for the sake of brevity, that T *contracts* E into the point P'. This expression, when used in this paper, will therefore always mean a little more than what it actually says; it will mean that not only does every point of E correspond to the point P' in the birational transformation T, but also that no point of F which lies outside the curve E corresponds to P' (and it is also tacitly assumed that P' is a normal point of F').

If a birational transformation $T: F \rightarrow F'$ contracts a curve E into a (normal) point P' of F' then we shall say that P' *is a contraction of* E. If, furthermore, T is regular at each point of E then we say that P' *is a regular contraction of* E.

An exceptional curve on a normal surface F is therefore a curve which admits a *simple contraction* (i.e., a contraction P' which is a simple point), and an exceptional curve of the first kind is one which admits a *simple regular contraction.* On the other hand, if E is an exceptional curve of F, *of the second kind,* then *any* birational transformation T of F which contracts E to a *simple* point has necessarily at least one fundamental point *on the curve* E (since F is normal), and thus T "blows up" some points of E into a curve.

PROPOSITION 2.3. *If P' is a simple regular contraction of an exceptional curve E, of the first kind, of a normal surface F, then P' is the only regular contraction of E (in the biregular sense; i.e., if P'' is any regular contraction of E then the local rings $\mathfrak{o}_{P'}$ and $\mathfrak{o}_{P''}$ coincide). Similarly, P' is the only simple contraction of E. The point P' is thus uniquely determined by the curve E, being independent of the choice of the birational transformation which contracts E into a simple point. The local ring $\mathfrak{o}_{P'}$ is the intersection of the local rings $\mathfrak{o}_P$, $P \in E$* (see IP, Theorem II.2.3).

It can be shown by examples that an exceptional curve of the first kind has infinitely many non-regular (and therefore necessarily non-simple, by Proposition 2.3) contractions. As to exceptional curves of the second kind, it can be shown that any such curve has infinitely many simple contractions (IP, Corollary II. 5.15).

Let E be an exceptional curve of the first kind on a *non-singular* surface F, and let $T: F \rightarrow F'$ be a birational transformation of F which contracts E to a simple point P'. By Proposition 2.3, the birational transformation T is necessarily regular at each point of E, whence P' is the (uniquely determined) simple regular contraction of E. Nothing in our definition of exceptional curves of the first kind specifies the behavior of T at points of F which are not on E. Thus T may have fundamental points outside of E; T may also contract into points other curves of F (such curves will necessarily have no point in common with E, since E is the *total* T^{-1}-transform of P' and since T is regular, hence single-valued, at each point of E; and the contractions of these curves will necessarily all be different from P'). However, it can be shown that there exists another birational transformation of F which contracts E to P' *and which is biregular on* $F - E$ (see IP, Theorem II. 2.4, where a more general result is proved). We can formulate this result in the following fashion:

We note first that $F - E + P'$ is easily seen to be an abstract surface in the sense of Weil. Then the above result can be stated as follows:

PROPOSITION 2.4. *If E is an exceptional curve, of the first kind, on a non-singular surface, and if P' is the (uniquely determined) simple (whence also regular) contraction of E, then the abstract surface $F - E + P'$ is a projective surface.*

By repeated applications of Proposition 2.4 we find the following generalization:

PROPOSITION 2.5. *If $E_1, E_2, \cdots, E_s$ are exceptional curves, of the first kind, on a non-singular surface F, such that no two of the curves E_i have points in common, and if P'_i is the simple contraction of E_i, then the abstract surface $F - \sum E_i + \sum P'_i$ is projective.*

The simplest exceptional curve of the first kind which has a preassigned contraction P', where P' is a simple point of a surface F', is the total transform of P' under a locally quadratic transformation of F' with center P'. The exceptional curve E which is thus obtained is irreducible, rational, non-singular, and its numerical characters $p(E)$ (arithmetic genus) and (E^2)

(virtual degree, or self-intersection number) are given by (see IP, Proposition II. 5. 9)

$$(1) \qquad p(E) = 0, \qquad (E^2) = -1.$$

Conversely, every irreducible exceptional curve E of the first kind, on a non-singular surface, is the total quadratic transform of its simple construction P' (IP, Corollary II. 3. 2). A deeper result is the following: if an irreducible curve E on a non-singular surface is such that $p(E) = 0$ and $(E^2) = -1$, then E is an exceptional curve of the first kind (see our Ergebnisse monograph "Algebraic surfaces" [11], pp. 71-72).

In IP we have derived a number of properties of reducible exceptional curves, of the first kind, on a non-singular surface (IP, Section II. 3), but we shall make no use of reducible exceptional curves of the first kind in the present paper.

Given a reducible exceptional curve E, of the first kind, on a non-singular surface F, it is possible to define a divisorial cycle $\mathcal{E}$ on F whose prime components are the irreducible components of E, counted to suitable (positive) multiplicities, in such way that relations similar to (1) be satisfied, i. e., so as to have $p(\mathcal{E}) = 0$ and $(\mathcal{E}^2) = -1$. For the definition and properties of these *exceptional cycles of the first kind* (which were not treated in IP) see our cited monograph [11], pp. 36-40; compare also our forthcoming note "Exceptional cycles of the first kind on a non-singular surface and the descending chain condition in birational classes of non-singular surfaces" in the Mem. Coll. Sci. Univ. Kyoto.

We terminate this section with listing a few properties of exceptional curves of the second kind, on a non-singular surface.

PROPOSITION 2. 6. *If a relatively minimal model carries an exceptional curve of the second kind, then it also carries an irreducible exceptional curve of the second kind.* (IP, Corollary II. 4. 6)

PROPOSITION 2. 7. *If E is an irreducible exception curve of the second kind, on a non-singular surface F, and if $s_1, s_2, \cdots, s_m$ are the multiplicities of its singular points (including its infinitely near singular points; if E is non-singular we set m and all the s_i equal to zero), then there exists a non-negative integer n such that*

$$(2) \qquad p(E) = \sum s_i(s_i - 1)/2,$$

$$(3) \qquad (E^2) = -1 + \sum s_i^2 + n, \quad n + m > 0; \; n, m \geqq 0.$$

It follows, in particular, that $(E^2) \geqq 0$ and that if E has singularities then $(E^2) > 0$. (IP, Corollary II. 5. 14)

We now prove the converse of Proposition 2.7:

PROPOSITION 2.8. *Let E be an irreducible curve on a non-singular surface F, and let $s_1, s_2, \cdots, s_m$ be the multiplicities of its singular points (including its infinitely near singular points). If there exists an integer $n \geqq 0$ such that $n + m > 0$ and such that the numerical characters $p(E)$ and (E^2) of E are given by* (2) *and* (3), *then E is an exceptional curve of the second kind.*

Proof. We have only to show that there exists an *antiregular* birational transformation $T: F \rightarrow F'$ of F onto a non-singular surface F' (i.e., a *transformation T such that T^{-1} is regular*) such that the *proper* transform $E' = T[E]$ of E is an exceptional curve of the first kind. For assume that this has already been shown. Then, denoting by P'' the simple contraction of E', the antiregularity of T shows immediately that the total transform of P'' *on F* contains the curve E and no other *curves.* Since the proper transform of P'' must be pure one-dimensional, it follows that E is the proper transform of P'', whence E is an exceptional curve. Since $(E^2) \geqq 0$, by (3), E must be of the second kind.

Now, to obtain T we apply to F successive quadratic transformations whose centers are at the singular points of E and of the successive transforms of E, until we obtain a *non-singular* proper transform $\bar{E}$ of E. From (2) and (3) we obtain easily that $p(\bar{E}) = 0$, $(\bar{E}^2) = -1 + n$. We then choose n distinct points of $\bar{E}$ and we apply n quadratic transformations with these points as centers. The proper transform of $\bar{E}$ is then an irreducible curve E' such that $p(E') = 0$ and $(E')^2 = -1$, hence an exceptional curve of the first kind. Q.E.D.

If K is a canonical divisor on a non-singular surface F and Z is any divisorial cycle on F we set

$$\sigma(Z) = -(Z \cdot K). \tag{4}$$

It is known (see IP, II.5, formula (6)) that

$$\sigma(Z) = (Z^2) - 2p(Z) + 2. \tag{5}$$

It follows from (2) and (3) that if E is an irreducible exceptional curve, of the second kind, on F, then

$$\sigma(E) = 1 + n + \sum s_i \geqq 2. \tag{6}$$

Thus $(E \cdot K) < 0$. On the other hand, we have $(E^2) \geqq 0$ and hence $(E \cdot Z) \geqq 0$ for any divisorial cycle $Z \geqq 0$. Consequently, if i is any integer

$\geqq 1$ there cannot exist a divisorial cycle $\geqq 0$ which is linearly equivalent to iK. In other words, the multicanonical systems $|iK|$, $i = 1, 2, 3, \cdots$, do not exist. We have therefore

PROPOSITION 2.9. *If a non-singular surface F carries an irreducible exceptional curve E of the second kind, then all the plurigenera P_i of F ($i \geqq 1$; $P_1 = p_g$) are zero.*

Remark. What matters in the proof of Proposition 2.9 is not that E is an exceptional curve of the second kind but the fact that E is an irreducible curve such that $(E^2) \geqq 0$ and $\sigma(E) > 0$. Consequently, already the presence of such an irreducible curve E implies the vanishing of all the plurigenera.

3. Preliminary criteria of existence of minimal models and statement of the main results. Let F be a member of our birational class $\mathfrak{B}$, i.e., F is a non-singular projective model of the function geld Σ/k. If F carries an exceptional curve E, of the first kind, and if P' is the simple contraction of E, then, by Proposition 2.4, the class $\mathfrak{B}$ contains the surface $F - E + P'$ which is strictly dominated by F, and hence F is not a relatively minimal model of Σ/k. Conversely, if F is not a relatively minimal model of Σ/k, then exists a surface F' in $\mathfrak{B}$ such that $F' < F \neq F'$, the birational transformation $T: F' \rightarrow F$ has then necessarily a fundamental point P' on F', and the total transform $T\{P'\}$ is an exception curve on F, of the first kind (since T^{-1} is regular on F, and P' is a simple point). We have therefore

PROPOSITION 3.1. *A necessary and sufficient condition that a surface F in the birational class $\mathfrak{B}$ be a relatively minimal model of Σ/k is that F be free from exceptional curves of the first kind.*

We now prove

PROPOSITION 3.2. *A necessary and sufficient condition that a non-singular projective model F of Σ/k be a minimal model of Σ/k is that F be free from exceptional curves* (of the first *or* of the second kind).

Proof. The condition is obviously sufficient. Suppose now that F carries an exception curve E. Let $T: F \rightarrow F'$ be a birational transformation of F which contracts E into a simple point P'. By the theorem of reduction of singularities there exists a non-singular projective model F'' of Σ/k such that $F' \prec F''$. Since P' is a simple point of F' we can choose the resolving birational transformation $F' \rightarrow F''$ of F' in such a way that it be biregular at P'. Then also the birational transformation $F \rightarrow F''$ contracts E to the point P'. Thus $F \not\prec F''$, and since $F'' \in \mathfrak{B}$, F is not a minimal model of Σ/k. This completes the proof.

Let E_1, E_2 be two exception curves, of the first kind, on a non-singular surface F, and let P' and P'' be the simple contractions of E_1 and E_2 respectively. If $E_1 \subset E_2$, then it follows from the last part of Proposition 2.3 that $\mathfrak{o}_{P'} \supset \mathfrak{o}_{P''}$. (Note that also the converse is true, for if $\mathfrak{o}_{P'} \supset \mathfrak{o}_{P''}$ then every zero-dimensional valuation with center P' has necessarily center P'', and thus the total transform E_1 of P' on F is contained in the total transform E_2 of P''). It follows that the projective surface $F - E_1 + P'$ strictly dominates the projective surface $F - E_2 + P''$ (we assume, of course, that $E_1 \neq E_2$). By the descending chain condition in $\mathfrak{B}$ (Proposition 1.5) it follows therefore that F *cannot carry a strictly ascending chain* $E_1 \subset E_2 \subset E_3 \cdots$ *of exceptional curves of the first kind.* If, then, we call an exceptional curve E of the first kind *maximal* when E is not a proper subset of any other exceptional curve of the first kind, then we conclude that *any exceptional curve, of the first kind, on a non-singular surface* F *is contained in at least one maximal exceptional curve of the first kind.*

PROPOSITION 3.3. *A necessary condition that the field* Σ/k *have a minimal model is that every non-singular projective model* F *of* Σ/k *have the following three properties:*

(a) F *carries no exceptional curves of the second kind.*

(b) F *has only a finite number of exceptional curves of the first kind.*

(c) *Any two distinct maximal exceptional curves of the first kind have no points in common.*

A sufficient condition that Σ/k *have a minimal model is that there exist a non-singular projective model of* Σ/k *having properties* (a), (b) *and* (c).

Proof. Assume that Σ/k has a minimal model, say F^*. Let F be any non-singular projective model of Σ/k. We first show that F can carry only exceptional curves *of the first kind.* Let E be an exceptional curve on F and let $T: F \rightarrow F'$ be a birational transformation of F which contracts E to a simple point P' ($P' \in F'$). Without loss of generality we may assume that F' is a non-singular surface (see proof of Proposition 3.2). Let P be any point of E. Since P and P' are corresponding points under T, there exists a zero-dimensional valuation v of Σ/k having centers P and P' on F and F' respectively. Let P^* be the center of v on F^*. Since F^* is a minimal model we have $F^* \prec F$ and $F^* \prec F'$, whence $\mathfrak{o}_{P^*} \subset \mathfrak{o}_P$ and $\mathfrak{o}_{P^*} \subset \mathfrak{o}_{P'}$. From these inclusions and from the fact that P, P' are simple centers of one and the same valuation it follows by a known result (see Zariski [12], Lemma on p. 538, or also IP, proof of Theorem II. 1. 1) that either $\mathfrak{o}_P \subset \mathfrak{o}_{P'}$ or $\mathfrak{o}_{P'} \subset \mathfrak{o}_P$. The first inclusion is impossible since T^{-1} is not regular at P' (the point P' is fundamental for T^{-1}). Hence $\mathfrak{o}_{P'} \subset \mathfrak{o}_P$, and thus T is regular at P. Since P was any point of E, the curve E is exceptional *of the first kind,* by Definition 2. 1.

We have thus shown that F has property (a). Now let $P_1^*, P_2^*, \cdots, P_s^*$ be the fundamental points of the birational transformation $f\colon F^* \rightarrow F$ and let $E_i = f\{P_i\}$. The s curves E_i on F are exceptional of the first kind (we assume, of course, that $F \neq F^*$, and that therefore $s \geqq 1$, for otherwise conditions (b) and (c) are trivially satisfied), and *no two of these curves have points in common;* both these assertions follow from the regularity of f. Let E be any exceptional curve on F. We know already that E is of the first kind. Let P' be the simple contraction of E, let $F' = F - E + P'$ and let P^* be *the* point of F^* which corresponds to P' in the birational transformation $F' \rightarrow F^*$. Since $\mathfrak{o}_{P^*} \subset \mathfrak{o}_{P'}$ and P' is fundamental for the birational transformation $F' \rightarrow F$, it follows that *a fortiori* also P^* is fundamental for $f\colon F^* \rightarrow F$. Hence P^* is one of the points P_i^*, say $P^* = P_1^*$. Since $\mathfrak{o}_{P^*} \subset \mathfrak{o}_{P'}$, it follows, by a remark made earlier, that the total transform E_1 of P^* on F contains the total transform E of P' on F. We have therefore shown that every exceptional curve E, of the first kind, on F is contained in one of the s exceptional curves E_i. Hence F carries exactly s maximal exceptional curves of the first kind, and this proves (b). Since no two of E_i intersect, the necessity of the condition is established.[3]

Assume now that there exists a non-singular projective model F of Σ/k having properties (a), (b) and (c). Let $E_1, E_2, \cdots, E_s$ be the maximal exceptional curves, of the first kind, on F and let P_i^* be the simple contraction of E_i. Since no two of E_i intersect, the abstract surface $F^* = F - \sum E_i + \sum P_i^*$ is projective (Proposition 2. 5). We shall show that F^* is a minimal model of Σ/k.

Let F' be any non-singular projective model of Σ/k and let $f\colon F' \rightarrow F$ and $f^*\colon F' \rightarrow F^*$ be the birational transformations of F' onto F and F^* respectively. Let P' be any point of F'. If f is regular at P' then also f^* is regular at P' since $F^* \prec F$. If f is not regular at P', let $E = f\{P'\}$ be the exceptional curve on F which is the total f-transform of the fundamental point P' of f. The exceptional curve E is of the first kind, since F has property (a), and E is contained in one of the s maximal exceptional curves E_i, say $E \subset E_1$. Since P' and $P_1{}^*$ are the simple contractions of E and E_1 respectively, it follows from $E \subset E_1$ that $\mathfrak{o}_{P'} \supset \mathfrak{o}_{P_1{}^*}$. Thus also in this case the birational transformation $f^*\colon F' \to F^*$ is regular at the point P'. Since P' is any point of F', it follows that $F' \succ F^*$. Since F' is any non-singular projective model of Σ/k the assertion that F^* is a minimal model of Σ/k is established. This completes the proof of the proposition.

---

[3] We observe that even if there does not exist a minimal model the following is true for any non-singular projective model F of Σ/k: there does not exist on F an infinite set of exceptional curves of the first kind such that no two curves in the set intersect. This is a straightforward consequence of the descending chain condition in the class $\mathfrak{B}$.

Our principal object in this paper is the characterization of those function fields Σ/k of transcendence degree 2 which have no minimal model. This characterization is given by the following theorem (due to the Italian geometers Castelnuovo and Enriques in the classical case):

FUNDAMENTAL THEOREM A. *If the field Σ/k does not possess a minimal model then Σ is the field of rational functions of a ruled surface (or equivalently: Σ is a simple transcendental extension $\Omega(t)$ of a field Ω/k of algebraic functions of one variable).*

The converse of the fundamental theorem A is also true, but is trivial. For, if $\Sigma = \Omega(t)$ and if C denotes a non-singular curve such that $k(C) = \Omega$, then the direct product $C \times L$, where L is a projective line, is a non-singular projective model of Σ/k (the Segre variety of the pairs of points of C and L). The curves E on $C \times L$, given by $Q \times L$ $(Q \in C)$, are irreducible, non-singular, and we have $p(E) = 0$, $(E^2) = 0$. Hence each E is an exceptional curve of the second kind (Proposition 2.8), and therefore $\Omega(t)$ has no minimal model (Proposition 3.3).

We shall prove the fundamental theorem A in the following stronger form:

FUNDAMENTAL THEOREM B. *If a non-singular surface F carries an irreducible exceptional curve E of the second kind, then F is birationally equivalent to a ruled surface, and if, furthermore, $(E^2) > 0$ (in particular, if E has singular points; see Proposition 2.7) then F is a rational surface.*

The remainder of this paper is devoted to the proof of this theorem. In regard to this theorem we point out at this stage that if the theorem is true under the additional assumption that F is a relatively minimal model then it is true in general. For assume that the theorem has already been proved under the assumption that F is a relatively minimal model and let F any non-singular surface satisfying the conditions of the fundamental theorem B. By the descending chain condition in the birational class $\mathfrak{B}$ of F, there exists a relatively minimal model F^* in B such that $F^* \prec F$. Let $T: F \rightarrow F^*$ be the (regular) birational transformation of F onto F^*. We assert that E is not an exceptional curve of T, i.e., that $T\{E\}$ is not a point. For assume the contrary, and let $T\{E\}$ be a point P^* of F^*. Let P' be a simple contraction of E and let F' be a non-singular surface which carries the point P'. From the regularity of T and from the fact that E is the total transform of P' it follows that P^* is the only point of F^* which corresponds to the point P' in the birational transformation $F' \rightarrow F^*$. Hence $\mathfrak{o}_{P^*} \subset \mathfrak{o}_{P'}$. Since we have also $\mathfrak{o}_{P^*} \subset \mathfrak{o}_P$ for any point P of E, the argument developed in the first part of the proof of Proposition 3.3 shows that $\mathfrak{o}_{P'} \subset \mathfrak{o}_P$. This being true for every point P of E, P' is a simple *regular* contraction of E, in contradiction with the fact that E is an exceptional curve of the *second* kind. [What we have proved here is that no irreducible component of an exceptional curve of the first kind (in the present case—of $T^{-1}\{P^*\}$) can be an exceptional curve of the second kind.]

Let then $T\{E\} = E^*$, where E^* is an irreducible curve on F^*. From the regularity of T and from the irreducibility of E it follows that also E^* is an exceptional curve (every simple contraction of E is also a contraction of E^*). The regularity of T implies that $(E^{*2}) \geqq (E^2)$ (IP, II 5, formula (12)). Since $(E^2) \geqq 0$ it follows that also $(E^{*2}) \geqq 0$, and consequently E^* is of the second kind. If, furthermore, $(E^2) > 0$ then also $(E^{*2}) > 0$, F^* is rational, and so is F.

The proof of the fundamental theorem will be divided in several cases, according as (E^2) is zero or positive, and in the latter case according to the value of (K^2), where K is a canonical divisor. In view of what was just said above, we may assume, in any given case, that F is a relatively minimal model. In some cases this assumption will play a crucial role in the proof, while in other cases that assumption is not required and will in fact not be made.

4. Case $(E^2) = 0$. *Beginning with this section, and throughout the rest of the paper, we assume that the field Σ/k has no minimal model.* We fix a relatively minimal model F of Σ/k. The surface F must then carry an *irreducible* exceptional curve E, of the second kind (Propositions 3.1, 3.2 and 2.6). In this section we assume that F carries an irreducible exceptional curve E, of the second kind, such that $(E^2) = 0$. Then E is non-singular and $p(E) = 0$ (Proposition 2.7), whence E is a non-singular rational curve.

We proceed to prove that *any non-singular surface F which carries an irreducible non-singular rational curve E such that* $(E^2) \geqq 0$ (such a curve is in fact exceptional of the second kind; see Proposition 2.8) *is birationally equivalent to a ruled surface.*

We first consider the case $(E^2)=0$. By formula (5) of Section 2 we have $\sigma(E)=2$ and consequently $\sigma(nE)=2n$ for any integer n.

If Z is any divisorial cycle on F then by the Riemann-Roch theorem

(1) $$\dim|Z|\geqq\tfrac{1}{2}[\sigma(Z)+(Z^2)]+p_a-i(Z),$$

where $i(Z)=1+\dim|K-Z|$ and p_a is the arithmetic genus of F. If $Z\geqq 0$ then $i(Z)=0$ since the canonical system dos not exist on our surface F (see *Remark* following Proposition 2.9). Applying (1) to the cycle $Z=nE$ we find

(2) $$\dim|nE|\geqq n+p_a, \qquad n\geqq 0.$$

For any integer $n\geqq 1$ we have only the following two possibilities: (a) either E is a fixed component of $|nE|$, and in that case $\dim|nE|=\dim|(n-1)E|$, or (b) E is not a fixed component of $|nE|$, and in that case $\dim|nE|=1+\dim|(n-1)E|$, since $(E^2)=0$ and since therefore the trace of $|nE|$ on E consists only of the zero-cycle on E. Hence in both cases we have $0\leqq\dim|nE|-\dim|(n-1)E|\leqq 1$, and from this it follows, in view of (2) that *for large* n we have

(3) $$\dim|nE|=n+c,$$

where c is a constant, and

(4) $$\dim|nE|=1+\dim|(n-1)E|.$$

Since E is irreducible, it follows from (4) that for large n the system $|nE|$ has no fixed components. On the other hand, if $n>1$ the system $|nE|$ must be reducible since any two cycles in $|nE|$ which pass through a given point of F must have a common component (the intersection number $(nE\cdot nE)$ being zero)). Therefore, for large n, the system $|nE|$ is composite with a pencil, or else all the members of $|nE|$ are the p-folds of other cycles, where p is the characteristic of k (Theorem of Bertini; see IP, Theorem I.6.3). The second alternative is to be excluded, for if n is large, then also $|(n-1)E|$ has no fixed components and thus $|nE|$ contains a cycle of the form $E+D$, where $D\in|(n-1)E|$ and E is not a component of D, so that E is a simple component of that cycle. Therefore $|nE|$ is composite with a pencil (not neecssarily linear) and thus it is also composite with a (uniquely determined) irreducible pencil, say L_n. Since $nE\in|nE|$, some multiple of E, say s_nE, belongs to L_n. Then every cycle in $|nE|$ which contains E as component must contain E to multiplicity $\geqq s_n$. Since we have just seen that if n is large, then there exist cycles in $|nE|$ which contain E as a simple component, we conclude that $s_n = 1$, i. e., E itself is a member of the pencil L_n. Since E is irreducible and $(E^2) = 0$, E cannot belong to two distinct pencils. Hence L_n does not depend on n, and the systems $|nE|$, n large, are composite with one and the same irreducible pencil $L = L_n$.

We have thus found a pencil L on F one member of which, namely E, is a prime cycle whose arithmetic genus is zero. But then also the general cycle of L, over k, has arithmetic genus zero. By the theorem of Noether-Enriques (or as a consequence of the purely algebraic theorem of Tsen [8]),[4] it follows that F is birationally equivalent to a ruled surface.

The preceding proof is applicable also to the case $(E^2) > 0$ provided E is *non-singular*, and in that case the conclusion is that *the surface F is rational.* In fact, if $(E^2) = s > 0$, then after s quadratic transformations with center on E and the successive transforms of E we obtain a non-singular surface F' on which the proper transform of E is an irreducible, non-singular, rational surve E' such that $(E'^2) = 0$. By the preceding proof, E' is a member of a pencil L'. The corresponding pencil L on F has s base points $(s > 0)$ and is therefore a linear pencil (Schilling-Zariski [6]). Therefore also L' is a linear pencil, and F is a rational surface (the field Ω of footnote 4 is now a simple transcendental extension of k).

5. Case $(E\ ) > 0$. The vanishing of $p_a(F)$. We now assume that our relatively minimal model F carries an irreducible exceptional curve E, of the second kind, such that the self-intersection number (E^2) of E *is positive.* Our object in the rest of the paper is to prove that F is a rational surfaces. In this section we shall carry out a first step of the proof, namely, we shall show that the arithmetic genus p_a *of F is zero.*

We shall need the following lemma:

LEMMA 5.1. *Let $T: G \to G'$ be a rational regular transformation of a non-singular surface G onto a (not necessarily non-singular) variety G' of*

---

[4] The pencil L determines a subfield Ω of Σ/k, of transcendence degree 1. The fact that the general member of L/k has arithmetic genus zero signifies that if Ω is taken as ground field then Σ—a field of algebraic functions of *one* variable over Ω—has genus zero. Thus Σ/Ω has divisors of degree 2 (the anticanonical divisors of Σ/Ω), and the Riemann-Roch theorem yields a projective model C of Σ/Ω which is a conic, defined over Ω. Since k is algebraically closed, the theorem of Tsen guarantees the existence of a rational point of C, over Ω, and consequently C is birationally equivalent, over Ω, to a projective line. Hence Σ is a purely transcendental extension of Ω.

positive dimension (whence G' is either a surface or a curve). If E is an irreducible curve on F such that $T\{E\}$ is a point then $(E^2) \leqq 0$.

Proof. Let L be the linear system on G, free from fixed components, which corresponds to the system of hyperplane sections of G' (see IP, I.3 and I.5). Since T is regular, L has no base points. Since E is exceptional for T, the linear system $Tr_E L$ has dimension zero, i.e., this linear system consists only of one divisor (on E). This divisor must be the null divisor, for L has no base points. Hence $(D \cdot L) = 0$ for any cycle D in L. Furthermore, if $\dim L = m$ (where necessarily $m \geqq 1$), then L contains a linear subsystem L_1, of dimension $m - 1$, having E as fixed component. Fix a cycle $sE + \Delta$ in L_1, where $\Delta \geqq 0$, $s \geqq 1$ and where we assume that E is not a component of Δ. Then $(\Delta \cdot E) \geqq 0$, and since $(sE + \Delta \cdot E) = 0$, it follows that $(E^2) \leqq 0$, as asserted.[5]

We now go back to our relatively minimal model F.

PROPOSITION 5.2. *The irregularity q of F is zero ($q =$ dimension of the Albanese variety of F).*

Proof. Let A be the Albanese variety of F, let f be the canonical mapping of F into A and let $F' = f(F)$. Since F is non-singular it follows, by a well-known property of Abelian varieties (A. Weil, [9], Th. 6, p. 27) that the rational transformation f of F onto F' is regular. Since E is a rational curve and since A carries no rational curves, *the transform $f(E)$ of E must be a point* (for otherwise $f(E)$ would be a *curve,* which—by the theorem of Lüroth—would then be rational). Since $(E^2) > 0$, it follows from the preceding lemma that F' cannot have positive dimension. Hence F' is a point, and since F' generates A, also A is a point. Q. E. D.

In the classical case, Severi has proved, by an essentially algebraic method, the completeness of the characteristic series of any ample complete continuous system of curves on a surface F whose geometric genus p_g is zero (see Severi [7], Anhang F; see also our monograph [11], pp. 84-86, where the proof and references may be found). In other words, Severi has proved, in the classical case, the *equality* $q = p_g - p_a$ by algebraic methods, under the assumption $p_g = 0$. This equality, under the same assumption, has now been established also in the abstract case, and independent proofs have been given by Akizuki-Matsumura [1], Nakai [4], [5] and Matsumura-Nagata

---

[5] Note that if F' is a *surface* then one can conclude that $(E^2) < 0$. For in that case we have $m \geqq 2$, $\dim L_1 > 0$, and thus we can find a cycle $sE + \Delta$ in L_1 such that $\Delta > 0$. By the connectedness theorem (Zariski [13], Theorem 14, p. 77) it then follows that $(\Delta \cdot E) > 0$, whence $(E^2) < 0$.

[3]. Since we know that for our surface F we have $p_g = 0$ (Proposition 2.9), it follows from Proposition 5.2 that $p_a = 0$. This completes the preliminary step of our proof of rationality of F.

In view of the vanishing of p_a, the Riemann-Roch inequality on the surface F is now as follows:

$$\dim |Z| \geqq \tfrac{1}{2}[\sigma(Z) + (Z^2)] - i(Z), \tag{1}$$

where $i(Z) = 1 + \dim |K - Z|$ and $\sigma(Z) = -(Z \cdot K)$ (Z, a divisorial cycle; K, a canonical cycle). Since $p_g = 0$ we have $i(Z) = 0$ if $Z \geqq 0$.

We denote by Z' any cycle which is linearly equivalent to $Z + K$, whence $|Z'|$ is the so-called *adjoint system of* $|Z|$. We set

$$(K^2) = \nu. \tag{2}$$

Then

$$\sigma(Z') = \sigma(Z) - \nu, \quad (Z'^2) = (Z^2) + \nu - 2\sigma(Z), \quad i(Z') = 1 + \dim |-Z|.$$

Hence, applying (1) to Z' instead of to Z, and using the equality $\sigma(Z) = (Z^2) - 2p(Z) + 2$, we find

$$\dim |Z'| \geqq p(Z) - \dim |-Z| - 2, \tag{3}$$

and if $|Z|$ *contains positive cycles then*

$$\dim |Z'| \geqq p(Z) - 1, \qquad Z > 0. \tag{4}$$

6. The case $(E^2) > 0$, $(K^2) \leqq 0$. In this section we prove the fundamental theorem B under the assumptions that $(E^2) > 0$, $(K^2) \leqq 0$ and that F is a relatively minimal model.

We assert that *the linear system* $|E + nK|$ (*the n-th adjoint system of* $|E|$) *does not exist if n is large.* In fact, we have $\sigma(E) \geqq 2$ [see (6), § 2], i.e., $(E \cdot K) \leqq -2$, whence $(E + nK \cdot E) < 0$ if n is large. Hence, if the system $|E + nK|$ exists for large n, then that system would have the curve E (which is *irreducible*) as fixed component, in contradiction with the nonexistence of $|nK|$ (Proposition 2.9).

Let m be the smallest integer ($m \geqq 0$) such that $|E + mK|$ exists and $|E + (m+1)K|$ does not exist. Since $(mK \cdot mK) = m^2(K^2) \leqq 0$ while $(E^2) > 0$, we have $E + mK \not\equiv 0$. Hence the system $|E + mK|$ consists of positive cycles. Let Z be a positive cycle in that system, and let D be any prime component of Z. Since $|Z'|$ does not exist, *a fortiori* $|D'|$ does not exist. Hence by (4), § 5, we must have $p(D) = 0$. On the other hand, since $\sigma(Z) = \sigma(E) - m(K^2) > 0$ we must have $\sigma(D) > 0$ for at least one prime component D of Z. For such a D we have therefore $(D^2)+2>0$ (since $p(D)=0$). The case $(D^2)=-1$ is excluded since F carries no exceptional curves of the first kind. Hence $(D^2)\geqq 0$, and thus F is birationally equivalent to a ruled surface (§ 4). Since $p_a(F)=0$, F is rational.

7. Some general properties of surfaces with $p_a=P_2=0$ and $(K^2)>0$. In this section we consider a non-singular surface F for which the following conditions are satisfied: $p_a=P_2=0$ and $(K^2)>0$. We shall derive some general properties of such a surface and we shall use these properties in the rest of the paper.

We set $(K^2)=\nu$ and we denote by K_a any *anticanonical* cycle, i. e., any cycle of the form $-K$. We note first of all that

$$(1)\qquad p(K_a)=1.$$

This equality holds on *any* non-singular surface, for we have $\sigma(K_a)=-(K_a\cdot K)=(K_a{}^2)$, and (1) follows from (5), 2. From $\sigma(K_a)=\nu$ we find by (1), § 5:

$$(2)\qquad \dim|K_a|\geqq\nu\geqq 1,$$

since $i(K_a)=\dim|2K|+1=0$. Hence the anticanonical system $|K_a|$ exists and has positive dimension. *A fortiori*, all the multi-anticanonical systems $|nK_a|$ $(n>0)$ exist and have positive dimension. Therefore none of the multicanonical systems $|nK|$ $(n>0)$ exists, and thus all the plurigenera of F vanish.

Let Z be any divisorial cycle on F and let n be an integer >0. Assume that the system $|Z+nK|$ exists. Then if we fix a *positive* cycle K_a in $|K_a|$, the linear system $|Z|$ will contain a cycle which is $\geqq nK_a$. Since, for a given Z, this is not possible if n is large, it follows that *the system $|Z+nK|$ does not eixst if n is large.* Thus the process of successive adjunctions, applied to a cycle Z, always terminates after a finite number of steps.

LEMMA 7.1. *If D is an irreducible curve on F and $|D'|$ does not exist, then $p(D)=0$ (and hence D is a rational non-singular curve).*

Proof. By (4), § 5, the non-existence of $|D'|$ implies $p(D)\leqq 0$, and hence $p(D)=0$ since D is an irreducible curve.

LEMMA 7.2. *Let K_a be a positive anticanonical cycle. If K_a is not a prime cycle, then every prime component of K_a has arithmetic genus zero.*

Proof. Let D be a prime component of K_a and let $K_a=D+\Delta$, $\Delta>0$.

We have $|D'| = |K_a - \Delta + K| = |-\Delta|$. Hence $|D'|$ does not exist, and we can apply the preceding lemma.

PROPOSITION 7.3. *If* $|K_a|$ *contains a reducible linear subsystem* L, *of positive dimension, then* F *is a rational surface.*

Proof. The system L may have fixed components. Let B be the maximal fixed component of L and let L_1 be the system obtained from L by deleting the fixed cycle B (so that L_1 is a linear system of positive dimension and free from fixed components). Let the cycle A be defined as follows: 1) If L_1 is irreducible then A is a general cycle of L_1/k. 2) if L_1 is reducible, then L_1 is either composite with an irreducible pencil or the cycles of L_1 are all of the form p^eC, where C varies in an irreducible linear system M of positive dimension; in the first case, A shall be a general cycle of that pencil, in the second case it shall be a general cycle of the linear system M/k. In all cases, A is a prime cycle and is a component of a positive anticanonical cycle which is not prime. Therefore, by Lemma 7.2, we have $p(A) = 0$. We have thus on F either an irreducible linear system of positive dimension, whose general cycle A has arithmetic genus zero, in which case F is a rational surface, by the theorem of Noether-Enriques; or a pencil whose general member A has arithmetic genus zero. In the latter case, F must be birationally equivalent to a ruled surface, again by the theorem of NoetherEnriques. But since $p_a = 0$, this ruled surface is of genus zero, and so again F is rational.

8. Proof of Castelnuovo's criterion of rationality in the case $(K^2) \geqq 3$. We again assume that $p_a = P_2 = 0$ and we consider first the case $(K^2) = \nu \geqq 4$. We fix a rational point P of F, over k, and we denote by L the linear system of all cycles in $|K_a|$ which have at P a singular point (hence at least a double point). We have $\dim L \geqq \dim |K_a| - 3$, whence, by (2), § 7: $\dim L \geqq \nu - 3 \geqq 1$. If L is reducible, then F is rational (Proposition 7.3). Assume that L is irreducible. Since $p(K_a) = 1$ it follows that the general member of L/k is a rational curve (which, however, as a cycle has arithmetic genus 1). Let $T \colon F \to \bar{F}$ be a quadratic transformation of F, with center P. For every cycle D in L we have $T(D) = \bar{D} + 2\bar{E}$, where $\bar{E} = T\{P\}$ is the irreducible exceptional curve of the first kind created by T and where $\bar{D}$ is a positive cycle. As D varies in L, $\bar{D}$ varies in a linear system $\bar{L}$, of positive dimension, and since $p(D) = 1$ it follows at once that $p(\bar{D}) = 0$. Thus $\bar{F}$ carries a linear system (of positive dimension) of cycles having arithmetic genus zero, the general cycle of the system being prime. Hence $\bar{F}$, and therefore also F, is rational.

We consider now the case $\nu = 3$. By Proposition 7.3 we may assume that $|K_a|$ is irreducible (since $\dim |K_a| \geqq 3$). If r denotes the dimension of $|K_a|$, the system $|K_a|$ defines a rational transformation $T\colon F \rightarrow F'$ of F onto an algebraic variety F' of positive dimension $\leqq 2$, immersed in a projective space of dimension r, whose system of hyperplane sections corresponds to $|K_a|$. Since $|K_a|$ is not composite with a pencil, F' is a surface (not a curve). Since the degree of $|K_a|$ is the prime integer 3 and the dimension is $\geqq 3$, the system $|K_a|$ cannot be composite with any unramified involution. Hence, the function field $\Sigma = k(F)$ either coincides with the function field $k(F')$ or is a purely inseparable extension of $k(F')$, of degree 3. In the latter case, F' would be a surface of *order* 1, i.e., a plane, which is impossible, since F' does not lie in a projective space of dimension $< r$, and $r \geqq 3$. Hence $k(F) = k(F')$, and F' is *a surface of* order $\geqq 3$, *birationally equivalent to* F (it could be a surface of order < 3, for *a priori* $|K_a|$ may have base points; see, however, Lemma 9.1 in the next section). If F' is a surface of order < 3, or if F' is a cubic surface and $r \geqq 4$, then F' is rational [if $r \geqq 4$ then a central projection of F' transforms F' birationally onto a quadratic surface; actually, it can be shown that $r = 3$ (see Lemma 9.1 in the next section)]. If F' is a cubic surface in S_3 $(r = 3)$ then F' cannot be an elliptic cubic cone since $p_a(F) = 0$ and since F and F' are birationally equivalent. Hence F' is necessarily a rational surface. This completes the proof of Castelnuovo's criterion in the case $\nu \geqq 3$.

9. Proof of the fundamental theorem B in the case $(K^2) = 1$.

In this case we shall use the following result:

PROPOSITION 9.1. *Let F be a relatively minimal model of a field Σ/k of algebraic functions of two variables and assume that $p_a = P_2 = 0$ and that $(K^2) = \nu > 0$. If there exists on F a divisorial cycle which is not linearly equivalent to an integral multiple of K, F is rational.*

Proof. We first show that *F carries at least one irreducible curve having arithmetic genus zero.* Assume the contrary. Since there exist on F divisorial cycles which are not linearly equivalent to an integral multiple of K, there also exist positive divisorial cycles having this property. Fix one such positive cycle Z. Let D be a prime component of Z. Since, by assumption, $p(D) \geqq 1$, the adjoint system $|D'|$ exists (Lemma 7.1). *A fortiori*, also the adjoint system $|Z'|$ $(= |D' + Z - D|)$ exists. The system $|Z'|$ must contain positive cycles since $Z \not\equiv -K$. Obviously no cycle in $|Z'|$ can be linearly equivalent to an integral multiple of K. Therefore, replacing Z by a cycle belonging to $|Z'|$ and applying the same argument we deduce that also the second adjoint system $|Z''|$ $(=|Z'+K|)$ exists. Thus all the successive adjoint system $|Z+nK|$, $n=1,2,\cdots$, exist, and this is in contradiction with what has been shown in the beginning of Section 7.

The proposition will be established if we show that either F is rational or F carries an irreducible curve E such that $p(E)=0$ *and* $(E^2) \geqq 0$. For in the latter case F is birationally equivalent to a ruled surface (Section 4) and is therefore again rational, since $p_a = 0$.

Assume that for *any* irreducible curve E on F such that $p(E)=0$ we have necessarily $(E^2) < 0$, and therefore $(E^2) \leqq -2$ (since F—a relatively minimal model—carries no exceptional curves of the first kind (Proposition 3.1)). We fix an irreducible curve E on F such that $p(E)=0$. Since $(E^2) \leqq -2$, we have $\sigma(E) = (E^2) - 2p(E) + 2 \leqq 0$, i.e., $(E \cdot K_a) \leqq 0$. If $(E \cdot K_a) < 0$, then E is a fixed component of $|K_a|$, thus $|K_a|$ is reducible and F is rational (Proposition 7.3). We are trus led to the only remaining possibility: if E is any irreducible curve on F such that $p(E)=0$ then $(E^2) = -2$, whence $\sigma(E) = (K_a \cdot E) = 0$. If we fix such a curve E, it is a fundamental curve of $|K_a|$ (in view of $(K_a \cdot E) = 0$). Thus there exist a cycle $\bar{K}_a$ in $|K_a|$ which has E as component. For *every* irreducible component $\bar{E}$ of $\bar{K}_a$ we have $p(\bar{E}) = 0$ (Lemma 7.2), whence $\sigma(\bar{E}) = 0$. This is in contradiction with $\sigma(\bar{K}_a) = \nu > 0$ and with the additive property of the numerical character σ. This completes the proof of the proposition.

Using the above proposition we shall now prove the fundamental theorem B in the case $(K^2) = 1$ assuming—as we may—that F is a relatively minimal model. It will be sufficient to show that our (irreducible) exceptional curve E of the second kind cannot be linearly equivalent to an integral multiple of K. Assume the contrary: $E \equiv qK_a$, where q is necessarily a positive integer since $|K_a|$ contains positive cycles. Then $(E^2) = q^2$ and $\sigma(E) = q$. Using formulae (2) and (3) of Section 2 (Prop. 2.7) we find

$$q^2 = -1 + \sum_{i=1}^{h} s_i^2, \qquad q = 1 + \sum_{i=1}^{h} s_i,$$

where $h > 0$, $s_i > 0$ $(i = 1, 2, \cdots, h)$ and where, in the notations of Proposition 2.7, we have set $h = n + m$ and $s_{m+1} = s_{m+2} = \cdots = s_h = 1$. Hence $(1 + \sum_{i=1}^{h} s_i)^2 = \sum_{i=1}^{h} s_i^2 - 1$, or $1 + \sum_{i<j} s_i s_j + \sum s_i = 0$, which is impossible.

10. Proof of Castelnuovo's criterion of rationality in the case $(K^2)=2$. We shall need the following lemma which deals with the general case of a non-singular surface F for which $p_a=P_2=0$ and ν $[=(K^2)]$ is an arbitrary positive integer.

LEMMA 10.1. *Let F be a non-singular surface such that $p_a=P_2=0$ and $\nu=(K^2)>0$. Then either F is rational or the following is true: the linear system $|K_a|$ is irreducible, $\dim|K_a|=\nu$ and, furthermore, if $\nu\geqq 2$, then $|K_a|$ has no base points and no fundamental curves.*

Proof. If $|K_a|$ is reducible, then F is rational (Proposition 7.3). Assume that $|K_a|$ is irreducible. We show that the assumption $\dim|K_a|>\nu$ leads to a contradiction, and that consequently $\dim|K_a|=\nu$, by (2), § 7. If $\dim|K_a|>\nu$, then the characteristic series of $|K_a|$ on a general member K_a^0 of $|K_a|/k$ is a linear series of degree ν and of dimension $\geqq\nu$ (hence necessarily of dimension ν, so that $\dim|K_a|=\nu+1$). This implies that K_a^0 must have a singular point Q. But then the cycles of $|K_a|$ which pass through Q would cut out on K_a^0 a linear series of degree $\leqq\nu-2$ and of dimension $\geqq\nu-1$, which is impossible.

Assume now that $\nu\geqq 2$ (and that $|K_a|$ is irreducible). If $|K_a|$ has base points, then the characteristic series of $|K_a|$ on K_a^0, after the fixed cycle at the base points has been deleted, would be a linear series L of degree $<\nu$ and of dimension $\nu-1$. Thus again K_a^0 would be of effective genus zero and would have to have a singular point Q. The point Q cannot be a base point, for in the contrary case the above series L would be actually of degree $\leqq\nu-2$ (and of dimension $\nu-1$), which is impossible. This being so, the cycles of $|K_a|$ which pass through Q would cut out on K_a^0, outside the fixed cycle at the base points *and* at Q, a series L_1 of degree $\leqq\nu-3$ and of dimension $\nu-2$, which again is impossible (note that L_1 is defined, since $\nu\geqq 2$ and since therefore $\dim|K_a|\geqq 2$, so that there exist cycles in $|K_a|$, *different from* K_a^0, which pass through Q).

Assume now that $|K_a|$ has fundamental curves (always under the assumption that $\nu\geqq 2$) and that $|K_a|$ is irreducible, and let Γ be an irreducible fundamental curve of $|K_a|$. Then there exist cycles D in $|K_a|$ which contain Γ as component, and these cycles form a linear system of dimension $\nu-1>0$. Therefore F is rational (Proposition 7.3). This completes the proof of the lemma.

The following is a generalization of the preceding lemma:

LEMMA 10.2. *Under the same assumptions as those of Lemma 8.1, either F is rational, or for any integer $n>1$ the following is true: the system*

$|nK_a|$ is irreducible, has dimension $\frac{1}{2}[\nu n(n+1)]$, is free from base points, and furthermore it is also free from fundamental curves if $\nu \geqq 2$ or if F is a relatively minimal model.

Proof. We may assume that $|K_a|$ is irreducible (otherwise F is rational). Applying the Riemann-Roch inequality (1), Section 5, to the cycle $Z = nK_a$, we find

$$\dim |nK_a| \geqq \tfrac{1}{2}[\nu n(n+1)]. \tag{1}$$

From the irreducibility of $|K_a|$ and from the fact that $\dim |K_a| > 0$, it follows that $|nK_a|$ can mave no fixed component. If $\nu > 1$ that $\dim |K_a| \geqq 2$ and hence $|nK_a|$ cannot be composite with a pencil. If $\nu = 1$ then $|K_a|$ is a pencil, and this could be the only irreducible pencil with which $|nK_a|$ might be composite. But were $|nK_a|$ composite with the pencil $|K_a|$, then we would have $\dim |nK_a| \leqq n$, in contradiction with (1) which yields $\dim |nK_a| \geqq \frac{1}{2}[n(n+1)] > n$ if $n > 1$. Hence $|nK_a|$ is not composite with a pencil. It is also clear that not all the cycles in $|nK_a|$ are p-folds of other cycles, for $|nK_a|$ contains sums of n distinct primes cycles belonging to $|K_a|$. We therefore conclude that $|nK_a|$ is irreducible.

We shall now prove, by induction on n, that $\dim |nK_a| = \nu n(n+1)/2$. Since this equality is valid for $n = 1$ (by the above Lemma 10.1), we assume $n \geqq 2$. We denote by r the dimension of the linear series $g = Tr_C |nK_a|$, where C is a general member of $|K_a|/k$. Then g is a series of degree $n\nu$, and we have $\dim |nK_a| = 1 + r + \dim |(n-1)K_a|$, whence, by induction hypothesis, $\dim |nK_a| = 1 + r + \frac{1}{2}[\nu n(n-1)]$. By (1) we must have $r \geqq \nu n - 1$. Were $\dim |nK_a| > \frac{1}{2}[\nu n(n+1)]$, we would have $r \geqq \nu n$, and the linear series g would have degree νn *and* dimension νn. That would imply that C has effective genus zero. Since $p(C) = 1$ [see (1), § 7], C would have to have a double point Q. The linear series cut out on C by the cycles of $|nK_a|$ passing through Q would then have degree $\leqq \nu n - 2$ and dimension $\geqq \nu n - 1$, which is impossible.[6] This proves the equality $\dim |nK_a| = \nu n(n+1)/2$.

If $\nu \geqq 2$, then $|K_a|$ has no base points or fundamental curves, and this implies that also $|nK_a|$ has this same property. In the case $\nu = 1$ we use an indirect argument. Assume that $|nK_a|$ has a base point A $(n \geqq 2)$.

---

[6] Note that the cycles in $|nK_a|$ which pass through the point Q form a linear system of dimension $\geqq \nu n(n+1)/2 - 1$, while the cycles in $|nK_a|$ which contain C as component form a linear system of dimension $\nu n(n-1)/2$. If $n \geqq 2$ the former dimension is greater than the latter, and thus there exist cycles in $|nK_a|$ which pass through Q and do not contain C as component. Therefore the linear series in question is defined.

Then A is also a base point of $|K_a|$, $A \in C$, and the series $g = Tr_C\,|nK_a|$, outside of a fixed cycle at A, has degree $\leqq n-1$. Since the dimension r of g is $n-1$, C is of effective genus zero and must have a double point Q. The point Q is different from A, for otherwise the above series g, outside a fixed cycle at A, would have degree $\leqq n-2$ and dimension $n-1$, which is impossible. The cycles of $|nK_a|$ passing through Q would cut out on C a series of degree $\leqq n-3$ and of dimension $n-2$, which is impossible.

For any irreducible fundamental curve E of $|nK_a|$, $n > 1$, we must have $(nK_a \cdot E) = 0$, since $|nK_a|$ has no base points. This implies that E is not linearly equivalent to any integral multiple of K_a. Hence if F is relatively minimal model, F is rational (Proposition 9.1).

This completes the proof of the lemma. Note that Proposition 9.1 has been used only at the end of the proof, and hence only in the case $\nu = 1$, since in the case $\nu \geqq 2$ the non-existence of fundamental curves of $|nK_a|$ has already been established in the earlier part of the proof.

After these preliminaries we begin to treat the case $\nu = 2$. We assume that we have a surface F which is a relatively minimal model of Σ/k and that we have $p_a = P_2 = 0$, $(K^2) = 2$. We also assume that $|K_a|$ is irreducible (Proposition 7.3). Then $|K_a|$ has no base points and has dimension 2 (see proof of Lemma 10.1). We may also assume that $|K_a|$ has no fundamental curves, for otherwise F is rational (Lemma 10.1) and there is nothing to prove.

Under these assumptions a very short proof of the rationality of F can be given, *provided the characteristic p is different from* 2. The proof is as follows:

The irreducible net $|K_a|$ defines a rational transformation $T: F \rightarrow S_2$ of F onto a projective plane, the T-transform of $|K_a|$ being the net of lines in S_2. Since $|K_a|$ has no base points, T is regular on F. Since $|K_a|$ has degree 2, the functions field Σ $(= k(F))$ is an algebraic extension, of degree 2, of the subfield $\Omega = k(S_2)$. Since $|K_a|$ has no fundamental curves, T^{-1} has no fundamental points in S_2. Since F is non-singular, it follows that *F is the normalization of S_2 in the field Σ* (F is a "double plane"). Since $p \neq 2$, the quadratic extension $\Sigma/k(S_2)$ is separable, and if x, y are affine coördinates in S_2, then the portion of F which lies over the affine (x, y)-plane is biregularly equivalent to a surface given by an equation of the form $z^2 = f(x, y)$, where $f(x, y)$ is a polynomial *free from multiple factors*. The curve $f(x, y) = 0$ is the affine part of the branch curve Δ of the double plane F. It follows from the equation $z^2 = f(x, y)$ that if l is a line in S_2 and C is the corresponding cycle in $|K_a|$ then a singular point of C necessarily corresponds to a multiple intersection of l with Δ. It follows that the general cycle in $|K_a|$ is a *non-singular* curve and is therefore of effective genus 1 (since $p(K_a)=1$). Since in an elliptic function field any function of order 2 has 4 branch points (provided the characteristic p is $\neq 2$), it follows that the branch curve Δ is of order 4. There exists at least one line l_0 in S_2 *which has no simple intersections with* Δ (this is an elementary fact from the theory of plane quartic curves). Then the corresponding cycle C_0 of $|K_a|$ will either have two double points or a tacnode (according as l_0 has two distinct intersections with C_0, both of multiplicity 2, or a single intersection of multiplicity 4); in both cases C_0 has the "equivalent" of *two* double points and therefore degenerates, i. e., C_0 is not a prime cycle. A prime component of C_0 cannot be linearly equivalent to an integral multiple of C_0, and therefore F is rational, by Proposition 9.1.

The above proof is not applicable to the case $p=2$. We shall now give another proof which is valid for any characteristic. This second proof is "constructive," for in it the surface F is explicitly constructed as a member of an algebraic system of surfaces having $p_a=P_2=0$ and $(K^2)=2$.

By Lemma 10.2 we have

$$\dim|2K_a|=6, \qquad \dim|4K_a|=20. \tag{2}$$

We fix a prime cycle C_0 in $|K_a|$, defined over k. The functions ξ in Σ such that $(\xi)+C_0>0$ form a vector space (over k) of dimension 3 (since $\dim|K_a|=2$), and 1 is one such function. We fix two elements x,y in Σ such that $\{1,x,y\}$ is a basis of that vector space. From what was said above in the course of the proof of rationality of F in the case $p\neq 2$, Σ is a quadratic extension of $k(x,y)$, and x,y are affine coördinates of the projective plane S_2 of which F is the normalization (in Σ). Clearly, Σ is a simple extension of $k(x,y)$. We shall now introduce a particular primitive element of $\Sigma/k(x,y)$.

The functions ξ in Σ such that $(\xi)+2C_0>0$ form a vector space (over k) of dimension 7 (since $\dim|2K_a|=6$, by (2)). The 3 functions $1,x,y,x^2,xy,y^2$ belong to that space and are linearly independent over k. Let z be a function in that vector space which is linearly independent of the above 6 functions. *We assert that z is a primitive element of $\Sigma/k(x,y)$.*

We first show that *z is an integral function of x and y.* For this purpose we have only to show that if $\mathfrak{p}$ is any algebraic place of Σ/k such that $\mathfrak{p}(x)$ and $\mathfrak{p}(y)$ are both finite then also $\mathfrak{p}(z)$ is finite. Let P be the center of $\mathfrak{p}$ on F. It will be sufficient to show that $P\notin C_0$, since C_0 is the only polar prime divisor of the function z. Assume the contrary: $P\in C_0$. Let

$(x) = C_1 - C_0$, $(y) = C_2 - C_0$, where $C_1, C_2 \in |K_a|$. Since $\mathfrak{p}(x) \neq \infty$, $\mathfrak{p}(y) \neq \infty$ and since $P \in C_0$, P necessarily belongs to C_1 and C_2. Since C_0, C_1, C_2 are three linearly independent cycles of the net $|K_a|$, P necessarily belongs to every cycle in $|K_a|$, i.e., P is a base point of $|K_a|$, in contradiction with the fact that $|K_a|$ has no base points.

To show that z is a primitive element of $\Sigma/k(x,y)$ we have only to show that $z \notin k(x,y)$. Assume the contrary. Then z is a polynomial $f(x,y)$ in x, y, since z is an integral function of x, y. Let n be the degree of the polynomial f. *We shall show that* $n \leqq 2$, and this will produce the desired contradiction, since the 7 functions $1, x, y, x^2, xy, y^2, z$ are linearly independent over k (by our choice of z).

Assume $n > 2$ and let $f_n(x,y)$ be the sum of terms of $f(x,y)$ which are of degree n. Since $f(x,y) - f_n(x,y)$ has order $\geqq -(n-1)$ on C_0 and $f(x,y)$ has order -2 on C_0, the quotient $f_n(x,y)/x^n$ must have positive order at the prime divisor C_0 (since $n > 2$). Hence, if we denote by c the C_0-residue of y/x then $f_n(1,c) = 0$, i.e., c is algebraic over k, and so $c \in k$ (note that $c \neq 0, \infty$ since both x and y have order -1 on C_0). The function $y - cx$ does not, therefore, become infinite at the prime divisor C_0 and thus has no polar prime divisors at all. Hence $y - cx \in k$, in contradiction with the linear independence of $1, x, y$ over k.

We have thus established that z is a primitive element of $\Sigma/k(x,y)$ (and, moreover, that it is an integral function of x, y).

To find the irreducible equation for z over $k(x,y)$ we consider the 22 monomials $x^m y^n$ $(0 \leqq m+n \leqq 4)$, $x^m y^n z$ $(0 \leqq m+n \leqq 2)$ and z^2, where m and n are non-negative integers. If ω is any of these monomials then $(\omega) + 4C_0 > 0$. Since $\dim |4K_a| = 20$ and since therefore the vector space of the functions ξ such that $(\xi) + 4C_0 > 0$ has dimension 21, it follows that *the above 22 monomials are linearly dependent over k.* The first 21 of those monomials (i.e., those which are different from z^2) are linearly independent over k (since x and y are algebraically independent over k and since $z \notin k(x,y)$). Hence the relation of linear dependence between the above 22 monomials has the following form:

$$z^2 + g_2(x,y)z + g_4(x,y) = 0, \tag{3}$$

where g_2 and g_4 are polynomials in x, y, of degree not greater than 2 and 4 respectively. The equation (3) is irreducible (since $z \notin k(x,y)$). We shall denote by g the polynomial on the left-hand side of (3) as well as the (projective) surface in S_3 defined by the equation (3). The surface g is birationally equivalent to F since $\Sigma = k(x,y,z)$. *We have therefore to prove the rationality of the surface g.*

We shall now make three remarks.

Remark 1. We denote by g_a the affine part of the surface, i.e., the set of points of g which are at finite distance in the (x, y, z)-space. We assert that *the affine surface* g_a *is normal.* To see this we have to show that $k[x, y, z]$ is the integral closure of $k[x, y]$ in Σ $(= k(x, y, z))$; or equivalently, that $\{1, z\}$ form an integral basis, over $k[x, y]$, of the integral closure of $k[x, y]$ in $k(x, y, z)$. Let ω be any function in $k(x, y, z)$ which is integral over $k[x, y]$. Since C_0 is the only polar curve of x and y on F, C_0 is also the only polar curve of ω on F. Hence there exists an integer $n \geqq 1$ such that $(\omega) + nC_0 \geqq 0$ (on F). Now, we have $\dim |nK_a| = n(n+1)$ [see (1)], and hence the vector space V of all functions ω in Σ such that $(\omega) +)nC_0 \geqq 0$ (on F) has dimension $n(n+1)+1$. On the other hand, the functions ζ of the form $f_n(x, y) + zf(x, y)$, where f_a and f_{n-2} are polynomials in x, y, of degree not greater than n and $n-2$ respectively, belong to that vector space. Since x, y are algebraically independent and since $z \notin k(x, y)$, the dimension of the space of functions ζ is $(n+1)(n+2)/2 + (n-1)n/2 = n(n+1)+1$. Hence this vector space coincides with V. Thus ω has the above form $f_n(x, y) + zf_{n-2}(x, y)$, and this proves our assertion.

Thus g_a is the normalization of the affine (x, y)-plane in the field Σ. Since F is the normalization of the *projective* (x, y)-plane in Σ, it follows that—up to biregular equivalence—the affine surface g_a can be identified with the part of the surface F which consists of those points P at which x and y are both finite (i.e., the point P of F such that $x, y \in \mathfrak{o}_P$). Since $(x) = C_1 - C_0$, $(y) = C_2 - C_0$, it follows that the part of F in question is $F - C_0$. *Thus* g_a *can be identified with* $F - C_0$.

If we now set $x' = 1/x$, $y' = y/x$, $z' = z/x^2$, then we find $(x') = C_0 - C_1$, $(y') = C_2 - C_1$, $(z') + 2C_1 > 0$. The three functions x', y', z' are connected by the equation

$$z'^2 + g'_2(x', y')z' + g'_4(x', y') = 0, \tag{3'}$$

where $g'_2(x', y') = x'^2 g_2(1/x', y'/x')$, $g'_4(x', y') = x'^4 g_4(1/x', y'/x')$. If we denote by g' the (projective) surface defined by (3′) and by g'_a the affine part of that surface (in the affine (x, y, z)-space), then we have, by a similar argument, that *the affine surface* g'_a *can be identified with* $F - C_1$.

Finally, if we set $x'' = x/y$, $y'' = 1/y$, $z'' = z/y^2$, then x'', y'', z'' are connected by the equation

$$z''^2 + g''_2(x'', y'')z'' + g''_4(x'', y'') = 0, \tag{3''}$$

where $g''_2(x'', y'') = y''^2 g_2(x''/y'', 1/y'')$, $g''_4(x'', y'') = y''^4 g_4(x''/y'', 1/y'')$, and the *affine* surface g''_a defined by (3″) can be identified with $F - C_2$. Since C_0, C_1, C_2 have no common points, it follows that *the three affine surfaces* g_a, g'_a, g''_a *cover* F.

Remark 2. The surface g is of order 4, unless g_4 is of degree $\leqq 3$ in which case g is of order $\leqq 3$. In the latter case the surface g is certainly rational since it cannot be an elliptic cubic cone (the birationally equivalent surface F having arithmetic genus zero). If g is a quartic surface, the point O at infinity on the z-axis is a double point of g. The plane sections of g passing through O have a tacnode at O (i. e., they have a double point infinitely near the double point O). This is easily seen by a direct analysis of the singular point O. [In the case of characteristic zero the general plane section of g through O is an elliptic quartic curve, since it corresponds birationally to a general anticanonical curve K_a on F. Since g has no singularities at finite distance (in view of the inclusion $g_a \subset F$) the general plane section of F has no singular points outside of O, and this shows again that O must be a tacnode of the section.] In other words, O is a tacnodal point of the surface g. The plane at infinity is the tangent plane of g at O, and the section of g with that plane decomposes into 4 lines through O (these are obtained by equating to zero the highest degree homogeneous component g_{44} of the polynomial $g_4(x,y)$). Conversely, it is easily seen that if a quartic surface in S_3 has a tacnodal point O then the equation of that surface takes the form (3) provided we take O as the point at infinity on the z-axis and take the tangent plane of the surface at O as the plane at infinity. The proof developed in this section will therefore establish the fact that *any quartic surface in* S_3 *which has a tacnodal point is either rational or is birationally equivalent to the ruled surface of genus* 1 (*say, an elliptic cubic cone*).

Remark 3. The linear system L on F which corresponds to the system of plane sections of g is defined by the 4 functions $1, x, y, z$. Since we have on F: $(x) = C_1 - C_0$, $(y) = C_2 - C_0$ and $(z) = D - 2C_2$, where $D \in |2K_a|$, L is generated by the 4 (linearly independent) cycles $2C_0, C_1 + C_0, C_2 + C_0, D$. (Note that L has no fixed components, since the *irreducible* curve C_0 cannot be a component of D; otherwise D would be of the form $C_0 + C_3$, where $C_3 \in |K_a|$, and D would belong to the system generated by $2C_0, C_1 + C_0$, $C_2 + C_0$, and this is not the case.) The base points of L are the 4 (generally distinct) intersections of C_0 and D. These intersections are the fundamental points of the birational transformation $T: F \rightarrow g$. To each of these points corresponds on g one of 4 lines in which the plane at infinity cuts g. The irreducible curve C_0 is a fundamental curve of L (since C_0 is a fixed component of the two-dimensional subsystem of L which is generated by the cycles $2C_0, C_1 + C_0, C_2 + C_0$). This curve C_0 is the only exceptional curve of T and to it corresponds on g the point O, which is thus a fundamental point of T^{-1}.. It is easily checked that O is the only fundamental point of T^{-1} and that the intersections of C_0 with D are the only fundamental points of T.

Note that the above considerations show that with our choice of C_0 (C_0-*irreducible*) the surface g must be of order exactly 4 (and not less), for L—a subsystem of the system $|2K_a|$, which has degree 8—has exactly 4 base points (or the equivalent of 4 base points if C_0 and D have some multiple intersections). The same conclusion holds true if C_0 is reducible, provided C_0 and D have no common components. Suppose, however, that C_0 is reducible and that one of its irreducible components, say Δ, is also a component of D. Then Δ is a fixed component of L, and the defining linear system of the birational transformation $T\colon F \rightarrow g$ is not L but the system L_1 obtained from L by deleting the fixed component Δ from all the cycles in L (we assume here, for simplicity, that L_1 has no fixed component). In this case it is easily found that L_1 has degree < 4, whence g is a surface of order $\leqq 3$. In this case, then, the rationality of F follows at once. We observe, however, that since we have assumed F to be a relatively minimal model, the rationality of F follows already, in view of Lemma 9.1, from the existence of a cycle $C_0 \in |K_a|$ which is not prime. (End of the remarks.)

As was stated at the end of Remark 2, we propose to prove in this section the following proposition:

PROPOSITION 10.3. *Every irreducible quartic surface g given by an equation of the form* (2) *is birationally equivalent to a cubic surface in S_3 (or to a surface of order < 3).*

This will establish Castelnuovo's criterion of rationality in the case $(K^2) = 2$, since every cubic surface, other than an elliptic cubic cone, is rational and since F—which has arithmetic genus zero—cannot be birationally equivalent to an elliptic cubic cone.

The intersection of the surface g with a plane is a cycle of degree 4. The proof of Proposition 10.3 will be based on the following lemma:

LEMMA 10.4. *If there exists a plane π through the tacnodal point O of g different from the plane at infinity, such that the intersection $g \cdot \pi$ splits into two cycles of degree 2, both passing through O, then the surface g is birationally equivalent to a surface of order $\leqq 3$.*

Proof. Let p_1, p_2, p_3, p_4 be the 4 lines in which the surface g is cut by the plane at infinity (the lines p_i need not be distinct). Subject to an affine change of the nonhomogeneous coördinates x and y, we may assume that π is the plane $x = 0$. Setting $g_2(0, y) = h_2(y)$, $g_4(0, y) = h_4(y)$, we see that the intersection cycle $g \cdot \pi$ consists of the cycle Γ defined by the equation

$$z^2 + h_2(y)z + h_4(y) = 0 \tag{4}$$

and perhaps of one (and only one) of the line p_i (counted to a suitable multiplicity). If $h_4(y)$ is of degree > 2 then equation (4) must be reducible, for otherwise Γ would be a prime cycle of degree $\geqq 3$, and the intersection cycle $g \cdot \pi$ could not split into two cycles of degree 2. Assume now that $h_4(y)$ is of degree $\leqq 2$. Then Γ is a cycle of degree 2, and Γ *does not pass through the point* O (the point at infinity on the z-axis). The intersection cycle $g \cdot \pi$ is then of the form $\Gamma + 2p_1$ (where p_1 is one of the lines p_i). Since $O \notin \Gamma$, $g \cdot \pi$ could not be a sum of two cycles of degree 2, both passing through O, unless Γ splits into two lines q_1, q_2 (in which case $g \cdot \pi$ has the desired decomposition $(q_1 + p_1) + (q_2 + p_1)$). Hence also in this case equation (4) must be reducible. Let then

$$z^2 + h_2(y)z + h_4(y) = (z + \psi(y))(z + \psi'(y)),$$

where $\psi(y)$ and $\psi'(y)$ are polynomials of degree $\leqq 2$. We now replace z by the element $z + \psi(y)$ (this amounts to a birational transformation $x' = x$, $y' = y$, $z' = z + \psi(y)$).[7] Then the equation (3) takes the form

$$z^2 + \bar{g}_2(x, y)z + x\bar{g}_3(x, y) = 0,$$

where $\bar{g}_2(x, y)$ and $\bar{g}_3(x, y)$ are polynomials of degree at most 2 and 3 respectively. Thus we may assume that *in the original equation* (3) *the polynomial* $g_4(x, y)$ *is divisible by* x. But then the birationally equivalent surface g' defined by equation (3′) (Remark 1) is a surface of degree $\leqq 3$ (since $g'_4(x', y')$ has now degree $\leqq 3$). This establishes Lemma 10.4.

The surface g belongs to an irreducible algebraic system N/k of quartic surfaces in S_3 whose general member G is defined by an equation of the form similar to (3):

$$G\colon z^2 + G_2(x, y)z + G_4(x, y) = 0,$$

---

[7] We observe—going back to the original surface F—that the conditions imposed on the element z (i.e., the divisor of the function z to be a mutiple of $-2C_0$ and z to be linearly independent of the functions $1, x, y, x^2, xy, y^2$) do not determine z uniquely. Any function of the form $cz + \psi(x, y)$, where $0 \neq c \in k$ and $\psi(x, y)$ is any polynomial of degree $\leqq 2$, will satisfy the same conditions.

where $G_2(x,y)$ and $G_4(x,y)$ are polynomials of degree 2 and 4 respectively, with coefficients which are algebraically independent over k. Note that $\dim N = 21$.

We shall prove that *there exists a plane* σ *such that* σ *and the intersection cycle* $G\cdot\sigma$ *satisfy the conditions of Lemma* 10.4 (*with* g *and* π *replaced by* G *and* σ). We assume for a moment that this assertion has already been proved and we show how Projosition 10.3 can be derived from this assertion.

The surface g is a specialization of G, over k. Let $(G,\sigma)\xrightarrow{k}(g,\pi)$ be an extension of the specialization $G\xrightarrow{k}g$. Then π is a plane through O, and since $G\cdot\sigma$ is a sum of two cycles of degree 2 passing through O, the same is true of the intersection cycle $g\cdot\pi$ (note that O is rational point over k). If π is not the plane at infinity, then Proposition 10.3 is established, in view of Lemma 10.4. If, however, π is the plane at infinity, then we replace both G and g by their birational transforms G' and g' under the transformation $x'=1/x$, $y'=y/x$, $z'=z/x^2$. Then also G' is a general member of N/k. Furthermore, if the equation of σ is $ax+by+c=0$ we denote by σ' the plane $a+by'+cx'=0$ (the transform of σ under the transformation $x'=1/x$, $y'=y/x$) and by π' the plane $x'=0$. It is clear that σ' and G' are in the same relationship to each other as are σ and G (i.e., the conditions of Lemma 10.4 are satisfied when g and π are replaced by G' and σ') and that (g',π') is a specialization of (G',σ') over k. Since π' is not the plane at infinity, g'—and therefore also g—is birationally equivalent to a surface of order $\leqq 3$. This completes the proof of Proposition 10.3.

We now proceed to the proof of the assertion that there exists a plane σ such that σ and the cycle $G\cdot\sigma$ satisfy the conditions of Lemma 10.4 (with g and π replaced by G and σ respectively).

The algebraic system N, of which G is a general member over k, contains an irreducible subsystem N' whose general member over k is the surface H defined by

$$(5)\qquad H:[z+\phi_2(x,y)]^2+A_2(x,y)[z+\phi_2(x,y)]+A_1(x,y)A_3(x,y)=0,$$

where A_1, A_2, A_3 and ϕ_2 are polynomials in x,y, of degree $1,2,3$ and 2 respectively, with coefficients which are algebraically independent quantities over k. We shall denote also by H the left-hand side of the equation (5). Then

$$(6)\qquad H=z^2+H_2(x,y)z+H_4(x,y),$$

where

$$(7)\qquad H_2(x,y)=A_2(x,y)+2\phi_2(x,y),$$

$$(8)\qquad H_4(x,y)=A_1(x,y)A_3(x,y)+A_2(x,y)\phi_2(x,y)+[\phi_2(x,y)]^2,$$

which shows that H is indeed a specialization of G over k and that consequently $N'\subset N$. Now, the surface H satisfies the conditions of Lemma 10.4 (with g replaced by H and π replaced by the plane $A_1(x,y)=0$), for the intersection of H with the plane $A_1(x,y)=0$ splits into two cycles of degree 2, defined respectively by the equations $z+\phi_2(x,y)=0$ and $z+\phi_2(x,y)+A_2(x,y)=0$, and both these cycles pass through the tacnodal point O. So everything will be proved if we show that *also the surface H is (as well as G) a general member of N/k* (and that therefore N' actually coincides with N).

From now on we shall denote by G^* (resp., H^*) the point, in the affine space of dimension 21, whose (non-homogeneous) coördinates are the coefficients of $G_2(x,y)$ and $G_4(x,y)$ (resp., of $H_2(x,y)$ and $H_4(x,y)$). We have $\dim G^*/k=21$, *and what we have to prove is that also*

$$(9)\qquad \dim H^*/k=21.$$

We shall denote by A^* (resp., ϕ^*) the point in the affine space of dimension 25 (resp., of dimension 6) whose (non-homogeneous) coördinates are the coefficients of the polynomials $A_1(x,y)$, $A_2(x,y)$, $A_3(x,y)$, $\phi_2(x,y)$ (resp., of the polynomial $\phi_2(x,y)$). We have $\dim A^*/k=25$, and we also know, by (7) and (8), that the point H^* is rational over the field $k(A^*)$. *Hence, in order to prove* (9), *we have to show* that

$$(10)\qquad \dim A^*/k(H^*)=4.$$

Since we have at any rate $\dim H^*/k\leqq 21$, it follows that $\dim A^*/k(H^*)\geqq 4$. So *all we have to prove is that*

$$(11)\qquad \dim A^*/k(H^*)\leqq 4.$$

Let A_1^* denote the point, in the affine 3-space, whose (non-homogeneous) coördinates are the coefficients of the linear polynomial $A_1(x,y)$ (note that this point is also rational over $k(A^*)$). We show first that

$$(12)\qquad \dim A^*/k(H^*,A_1^*)\leqq 3.$$

We fix a (finite) specialization $\bar{A}^*$ of A^* over $k(H^*,A_1^*)$ *which is algebraic over $k(H^*,A_1^*)$*. The coördinates of the point $\bar{A}^*$ are the coefficients of certain polynomials $\bar{A}_1(x,y)$, $\bar{A}_2(x,y)$, $\bar{A}_3(x,y)$ and $\bar{\phi}_2(x,y)$ (of indicated degrees). We have $\bar{A}_1(x,y) = A_1(x,y)$ since $\bar{A}^*$ is a specialization of A^* over $k(A_1^*)$. By (7) and (8) we have

$$H_2(x,y) = \bar{A}_2(x,y) + 2\bar{\phi}_2(x,y),$$

$$H_4(x,y) = A_1(x,y)\bar{A}_3(x,y) + \bar{A}_2(x,y)\bar{\phi}_2(x,y) + [\bar{\phi}_2(x,y)]^2, \tag{13}$$

whence upon setting

$$q_2(x,y) = \bar{\phi}_2(x,y) - \phi_2(x,y), \tag{14}$$

we find, again by (7) and (8):

$$A_2(x,y) = \bar{A}_2(x,y) + 2q_2(x,y), \tag{15}$$

$$A_1(x,y)A_3(x,y) = A_1(x,y)\bar{A}_3(x,y) + \bar{A}_2(x,y)q_2(x,y) + [q_2(x,y)]^2. \tag{16}$$

From (16) it follows that $q_2(x,y)$ must satisfy the congruence

$$\bar{A}_2(x,y)q_2(x,y) + [q_2(x,y)]^2 \equiv 0 \quad (\operatorname{mod} A_1(x,y)).$$

Since q_2 must be a polynomial of degree $\leqq 2$ this congruence has only two general solutions q_2^*; they are given by $q_2^*(x,y) = A_1(x,y)p_1(x,y)$ and $q_2^*(x,y) = -\bar{A}_2(x,y) + A_1(x,y)p_1(x,y)$ respectively, where $p_1(x,y)$ is the general linear polynomial in x, y. Each of these solutions depends on three arbitrary parameters; more precisely, we have $\dim q_2^*/k(H^*, A_1^*) = 3$ (note that the coefficients of $\bar{A}_2(x,y)$ are algebraic over $k(H^*, A_1^*)$, by our choice of the specialiaztion $\bar{A}^*$). From (14), (15) and (16) we see that the coefficients of ϕ_2, A_2 and A_3 are rational over $k(\bar{A}^*, q_2^*)$. Since $\bar{A}^*$ is algebraic over $k(H^*, A_1^*)$, it follows that A^* is algebraic over $k(H^*, A_1^*, q_2^*)$. The inequality (12) now follows from the equality $\dim q_2^*/k(H^*, A_1^*) = 3$.

In view of (12), the inequality (11) will be established if we show that

$$\dim A_1^*/k(H^*) \leqq 1. \tag{17}$$

It will be sufficient to show that the number of *planes* $\bar{A}_1(x,y) = 0$ (in the ambient 3-space of the surface H) such that the $\bar{A}_1(x,y)$ is a (finite) specialization (over $k(H^*)$, of the linear polynomial $A_1(x,y)$), is finite.

Now, any such plane shares with the plane $A_1(x,y) = 0$ the property that its intersection with the surface H splits into two cycles of degree 2, both passing through the tacnodal point 0 of H. Now, let $\bar{A}_1(x,y)$ be such a plane. The quadratic polynomial H in z factors, $\operatorname{mod} \bar{A}_1$, into a product $(z+\bar{\psi})(z+\bar{\psi}')$, where $\bar{\psi}$ and $\bar{\psi}'$ are polynomials in x, y, of degree 2 (see proof of Lemma 10.4). We have seen in the proof of Lemma 10.4 that the birational transformation

$$(18) \qquad \bar{x} = x/\bar{A}_1, \qquad \bar{y} = y/\bar{A}_1, \qquad \bar{z} = z + \psi/\bar{A}_1^2$$

transforms H into the cubic surface

$$C\colon \bar{z}^2 + C_2(\bar{x},\bar{y})z + C_3(\bar{x},\bar{y}) = 0,$$

where C_2 and C_3 are polynomials of degree 2 and 3 respectively. From the fact that A_1, A_2, A_3 and ϕ_2 are polynomials whose coefficients are algebraically independent over k it follows at once that C is the *general cubic surface* in S_3 (referred to a special system of coördinates). Now, it is clear that in the birational transformation (18) the system of plane section of H through O corresponds to the system of plane sections of C passing through the point at infinity on the $\bar{z}$-axis. If a plane π passing through O, different from the plane at infinity and the plane $\bar{A}_1 = 0$, intersects H in a sum of two cycles, of degree 2, both passing through O, then the section of C with the corresponding plane $\alpha\bar{x} + \beta\bar{y} + \gamma = 0$ is reducible and therefore contains a line of the cubic surface. Since the general cubic surface contains only a finite number of lines, the number of planes π with the above indicated property is finite. This completes the proof.

HARVARD UNIVERSITY.

REFERENCES.

[1] Y. Akizuki and H. Matsumura, "On the dimension of algebraic systems of curves with nodes on a non-singular surface," *Mem. Coll. Sci. Univ. Kyoto*, series A, vol. 30, n. 2 (1957), pp. 143-150.

[2] F. Enriques, *Le superficie algebriche*, Bologna, Zanichelli, 1949.

[3] H. Matsumura and M. Nagata, "On the algebraic theory of sheets of an algebraic variety," *Mem. Coll. Sci. Univ. Kyoto*, series A, vol. 30, n. 2 (1957), pp. 157-164.

[4] Y. Nakai, "A property of an ample linear system on a non-singular variety," *ibid.*, series A, vol. 30, n. 2 (1957), pp. 151-156.

[5] ———, "On the characteristic linear systems of algebraic families," forthcoming in the *Illinois Journal of Mathematics*.

[6] O. F. G. Schilling and O. Zariski, "On the linearity of pencils of curves on algebraic surfaces," *American Journal of Mathematics*, vol. 60 (1938), pp. 320-324.

[7] F. Severi, *Vorlesungen über algebraische Geometrie*, Teubner, Berlin, 1921.

[8] C. C. Tsen, "Divisionalgebren über Funktionenkörpern," *Nach. Ges. Wiss.*, Göttingen,1933.

[9] A. Weil, "Variétés abéliennes et courbes algébriques," *Actual. Scient. et Indust.*, n. 1064, Paris, 1948.

[10] ———, "Sur les critères d'équivalence en géométrie algébrique," *Math. Ann.*, vol. 128 (1954), pp. 95-127.

[11] O. Zariski, "Algebraic surfaces," *Ergebnisse der Mathematik und ihrer Grenzgebiete* 3, n. 5 (1935).

[12] ———, "Reduction of the singularities of algebraic three-dimensional varieties," *Annals of Mathematics*, vol. 45 (1944), pp. 472-542.

[13] ———, "Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields," Mem. Amer. Math. Soc., n. 5 (1951).

[14] ———, "Introduction to the problem of minimal models in the theory of algebraic surfaces," forthcoming in the *Publications of the Mathematical Society of Japan* (referred to as IP).

THE DETERMINATION OF PARACOMPACTNESS BY UNIFORMITIES.*[1]

By H. H. Corson.

1. Introduction.

In the theory of paracompact spaces the global nature of the concept of paracompactness is emphasized by many theorems. It would seem then that some convenient formulation would be possible in terms of uniform structures.

A possible solution to this problem was suggested by Kelley in [3, p. 208], where he conjectured that if X is topologically complete, plus another condition, then X is paracompact. This conjecture was shown by Isaac Namioka to be false. However, in the theorem proved below it will be seen that a property very similar to topological completeness is successful in this rôle. In fact X is paracompact if and only if X admits a uniformity under which every filter satisfying a Cauchy-like condition has a cluster point.

A well known open question which appears to be closely related to our theorem is this. If a topological space has the property that its product with every compact space is normal, is it paracompact? Dieudonné proved in [2] that every paracompact space X has this property, and also that the set of all neighborhoods of the diagonal is a uniformity for X. Our theorem demonstrates that, together at least, these two properties are sufficient as well as necessary.

However, since paracompact is a purely topological term, we give a formulation of our results in topological terminology. As might be expected from the theory of uniform structures, this last equivalence is between paracompact spaces and spaces on which enough continuous functions are defined, these functions taking values in metric spaces (metrizable spaces).

The last section of the paper is devoted to relating our theorem with known results. Some shortcomings of our methods are pointed out, as well as some applications. An example of the latter is the use of our theorem to

---

* Received September 5, 1957; revised December 12, 1957.

[1] Written with the support of the National Foundation grant to Tulane University.

compare paracompact spaces with topological spaces which are Lindelöf spaces, Q, or topologically complete.

2. The theorem. Before stating the theorem, we should first mention that the necessary termininology and theory of filters, uniform structures and paracompact spaces may be found either in Bourbaki [1] or Kelley [3]. We will also need to define the following property of a filter, which is slightly weaker than the Cauchy property.

Definition. A filter $\mathfrak{F}$ in a uniform space $(X, \mathfrak{U})$ is *weakly Cauchy* if for every $U \in \mathfrak{U}$ some filter stronger that $\mathfrak{F}$ becomes U small. That is there is a filter $\mathfrak{H}_U$, $\mathfrak{F} \subset \mathfrak{H}_U$, and $H \times H \subset U$ for some $H \in \mathfrak{H}_U$. All topological spaces will be assumed to be Hausdorff spaces.

THEOREM 1. *For a topological space X the following are equivalent:*

(a) *X is paracompact.*

(b) *The set of all neighborhoods of the diagonal is a uniformity for X, and the product of X with every compact space is normal.*

(c) *There is a uniformity for X under which every weakly Cauchy filter has a cluster point.*

(d) *If $\mathfrak{F}$ is a filter in X such that the image of $\mathfrak{F}$ has a cluster point in any metric space into which X is continuously mapped, then $\mathfrak{F}$ has a cluster point in X.*

Proof of (a) $\Rightarrow$ (*b*). This follows from the theorem of Dieudonné [2].

Proof of (b) $\Rightarrow$ (c). Assuming (b) we may choose a uniformity $\mathfrak{U}$ for X where $\mathfrak{U}$ is the set of all neighborhoods of the diagonal Δ. Suppose $\mathfrak{F}$ is a filter which is weakly Cauchy under $\mathfrak{U}$ and such that $\mathfrak{F}$ has no cluster point in X. Let A be the cluster points of $\mathfrak{F}$ in some compactification of X, say $\alpha(X)$. Then it is easily verified that Δ and $A \times X$ are disjoint closed sets in $\alpha(X) \times X$, and consequently by (b) there is a neighborhood U of Δ such that closure (U) does not intersect $A \times X$.

By our choice of $\mathfrak{U}$ we have that $U \in \mathfrak{U}$. Since $\mathfrak{F}$ is assumed weakly Cauchy, there is a filter $\mathfrak{H}$ stronger than $\mathfrak{F}$ with $H \in \mathfrak{H}$ and $H \times H$ contained in U. We now have this situation. $\mathfrak{H}$ has a cluster point in $\alpha(X)$, this cluster point is also a cluster point of $\mathfrak{F}$, and it clearly is not in A. This contradicts the assumption that A was the set of all cluster points of $\mathfrak{F}$.

Proof of (c) $\Rightarrow$ (*d*). Let $\mathcal{F}$ be a filter whose image has a cluster point in every metric continuous image of X. We assume that $\mathcal{U}$ has the property stated in (c) and prove that $\mathcal{F}$ is weakly Cauchy with respect to $\mathcal{U}$.

If $U \in \mathcal{U}$, then we must show there is an $\mathcal{H}$ stronger than $\mathcal{F}$ such that $\mathcal{H}$ becomes U small. However, by the characterization of $\mathcal{U}$ in terms of écarts, it follows that there is a pseudo metric p with $U' = \{(x, y) : p(x, y) \leqq 1\}$ contained in U. Furthermore, if $\mathcal{J}$ is the original topology for X, the identity map from $(X, \mathcal{J})$ to (X, p) is continuous; thus if Y is the metric space canonically associated with (X, p) then there is an induced map f from $(X, \mathcal{J})$ to Y.

From our assumptions on $\mathcal{F}$, $f(\mathcal{F})$ clusters in Y; therefore there is a filter $\mathcal{H}'$ stronger than $f(\mathcal{F})$ which converges in Y. It follows that $\mathcal{H} = \sup\{f^{-1}(\mathcal{H}'), \mathcal{F}\}$ is a filter which has the properties required. In fact since $\mathcal{H}'$ is Cauchy in Y, there is a $H' \in \mathcal{H}'$ such that $H' \times H'$ is contained in $f \times f(U')$. Thus for some $H \in \mathcal{H}$, $H \subset f^{-1}(H')$ and $H \times H \subset U' \subset U$.

Proof of (d) $\Rightarrow$ (a). Suppose X were not paracompact under the conditions in (d), then there is an open covering $\mathcal{O}$ of X with no locally finite open refinement.

Suppose $\boldsymbol{R}$ is the collection of finite subsets of $\mathcal{O}$, and for each $\mathcal{R} \in \boldsymbol{R}$ let $F(\mathcal{R})$ be the complement of $\bigcup\{R : R \in \mathcal{R}\}$. Obviously no finite subcollection of $\mathcal{O}$ covers X, therefore $\{F(\mathcal{R}) : \mathcal{R} \in \boldsymbol{R}\}$ is the base of a filter $\mathcal{F}$; and, since $\mathcal{O}$ is an open cover, $\mathcal{F}$ has no cluster point in X.

By hypothesis there is a continuous mapping f of X into a metric space M such that $f(\mathcal{F})$ has no cluster point in M. Let $\mathcal{U}$ be the open cover of M defined by $U \in \mathcal{U}$ if and only if U is the interior of the complement of some $f(F)$ with $F \in \mathcal{F}$. Since by A. H. Stone's theorem [6] each metric space is paracompact, there is a locally finite open refinement $\mathcal{V}$ of $\mathcal{U}$.

We now consider the cover $\mathcal{L}$ of X where $\mathcal{L} = \{f^{-1}(V) : V \in \mathcal{V}\}$. $\mathcal{L}$ is locally finite in X since $\mathcal{V}$ is locally finite in M. Moreover, $L \in \mathcal{L}$ implies L is in the complement of some $\mathcal{F}(\mathcal{R})$, so $\mathcal{R}(L) = \{L \cap R : R \in \mathcal{R}\}$ is a cover of L.

Let us show that $\mathcal{B} = \bigcup\{\mathcal{R}(L) : L \in \mathcal{L}\}$ is *a* locally finite open refinement of $\mathcal{O}$. $\mathcal{B}$ is obviously a cover of X, and each $L \cap R \in \mathcal{R}(L)$ is contained in some member of $\mathcal{O}$. To show that $\mathcal{B}$ is locally finite, fix $x \in X$ and a neighborhood U of x such that U intersects only a finite number of members of $\mathfrak{L}$. Since each of these L is covered by a finite number of $L \cap R$, we see that U intersects only a finite number of $C \in \mathfrak{C}$. This contradiction completes the proof.

3. Comments.

I. A space X may be defined to be topologically complete if it is complete under the strongest admissible uniformity $\mathfrak{U}$. Closely related to this (see [4] and [5]), X is Q if it is complete under the weakest uniformity $\mathfrak{V}$ such that all real valued continuous functions are uniformly continuous. Since (c) of Theorem 1 may be stated in terms of $\mathfrak{U}$, the following question arises. Which are the spaces such that every filter weakly Cauchy with respect to $\mathfrak{V}$ has a cluster point?

THEOREM 2. *For a regular topological space X the following are equivalent:*

(a) *X is a Lindelöf space.*

(b) *Every filter weakly Cauchy with respect to $\mathfrak{V}$ has a cluster point.*

(c) *If a filter $\mathfrak{F}$ is such that its image has a cluster point in the reals under every real continuous image of X, then $\mathfrak{F}$ has a cluster point in X.*

Proof of (a) $\Rightarrow$ (b). Let $\mathfrak{F}$ be a filter weakly Cauchy under $\mathfrak{V}$. Since X is a regular Lindelöf and hence normal, there is a filter $\mathfrak{H}$ weaker than $\mathfrak{F}$ such that (i) $\mathfrak{H}$ has a base of sets of the form $Z(f) = \{x : f(x) = 0\}$ and (ii) $\mathfrak{H}$ has the same cluster points as $\mathfrak{F}$.

Suppose $\mathfrak{F}$, and therefore $\mathfrak{H}$, has no cluster point. Then the hypothesis that X is Lindelöf implies the existence of a countagle collection of $Z(f_i) \in \mathfrak{H}$ such that $\cap Z(f_i)$ is empty. Since we may also assume $0 \leqq f_i \leqq 1$, we have that $g = (\sum_{1}^{\infty} 2^{-i} f_i)^{-1}$ is a real continuous function defined on all of X. Moreover, if $V = \{(x,y) : |g(x) - g(y)| \leqq 1\}$, then no filter stronger than $\mathfrak{F}$ can become V small.

Proof of (b) $\Rightarrow$ (c). The proof is entirely similar to that of (c) $\Rightarrow$ (d) in Theorem 1.

Proof of (c) $\Rightarrow$ (a). Let $\mathfrak{F}$ be a filter with no cluster point. By (c) there is a real map f such that $f(\mathfrak{F})$ has no cluster point in the real numbers. Let $F_n \in \mathfrak{F}$ be chosen with the property $|f(F_n)| \geqq n$. Then $\cap F_n$ is void, and thus X is Lindelöf.

II. Theorem 1 may be considered an extension of this known theorem (see [3], Chap. 6, Prob. T, or [1], Chap. 2, Sect. 4, Prob. 10). A locally compact space X is paracompact if (and only if) there is an entourage U in the strongest uniformity for X such that $U[x]$ is compact for every x. In fact, if a filter $\mathfrak{H}$, stronger than $\mathfrak{F}$, is eventually contained in the compact subspace $U[x]$ for some x, then $\mathfrak{H}$ and hence $\mathfrak{F}$ has a cluster point.

However, the following criterion of Kelley's should be mentioned in this connection: X is paracompact if and only if (K) given an open cover $\mathcal{O}$ of X there is a neighborhood D of Δ such that $\{D[x] : x \in X\}$ is a refinement of $\mathcal{O}$. One easily finds that (K) implies property (c) of Theorem 1, but the converse is perhaps most easily proved by first proving our Theorem.

III. It is obvious that every Cauchy filter is contained in a Cauchy ultrafilter, and from our theorem every filter weakly Cauchy under the strongest uniformity $\mathcal{U}$ on a paracompact space is contained in a weakly Cauchy ultrafilter. However, it is not even true in general that every weakly Cauchy filter is weaker than a maximal weakly Cauchy filter. The next theorem illustrates that it is precisely this failure which makes our result a theorem instead of a panacea.

First let us notice that a maximal weakly Cauchy filter (under $\mathcal{U}$) is either eventually in a set or eventually out of it, in fact it is an ultrafilter. Let A be a subset of X, $\mathfrak{F}$ a maximal weakly Cauchy filter in X, and suppose no $F \in \mathfrak{F}$ is contained in A or in its complement. Since $\mathfrak{F}$ is maximal there is a $U_1 \in \mathcal{U}$ such that no filter stronger than $\mathfrak{F} | A$ become U_1 small; and there is a U_2 having the same property with respect to $\mathfrak{F}$ restricted to the complement of A. It follows that no filter stronger than $\mathfrak{F}$ becomes $U_1 \cap U_2$ small, and thus a contradiction.

THEOREM 3. *A topologically complete space X is paracompact if and only if every filter in X, weakly Cauchy with respect to $\mathcal{U}$, is weaker than a maximal weakly Cauchy filter.*

The necessity is obvious, while the sufficiency follows from Theorem 1 and the above remarks. In fact an ultrafilter is Cauchy if it is weakly Cauchy.

We know from a theorem of Stone's [6] that the product P of more than a countable number of non-compact, paracompact spaces is not paracompact, but P is topologically complete. Thus there is not necessarily a supremum in a maximal tower of weakly Cauchy filters.

TULANE UNIVERSITY.

REFERENCES.

[1] N. Bourbaki, *Topologie Générale*, Paris, 1948.

[2] J. Dieudonné, "Une généralization des espaces compacts," *Journal de Mathématiques*, ser. 9, vol. 23 (1944), pp. 65-76.

[3] J. L. Kelley, *General Topology*, New York, 1955.

[4] L. Nachbin, "Topological vector spaces of continuous functions," *Proceedings of the National Academy of Sciences*, vol. 40 (1954), pp. 471-474.

[5] T. Shirota, "A class of topological spaces," *Osaka Mathematical Journal*, vol. 4 (1953), pp. 23-40.

[6] A. H. Stone, "Paracompactness and product spaces," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 977-982.

ON THE STRUCTURE OF ORTHOGONAL GROUPS.*

By TSUNEO TAMAGAWA.

Let V be a vector space over a field k and Q a quadratic form defined on V whose associated bilinear form $B(x,y)=Q(x+y)-Q(x)-Q(y)$ is nondegenerate. Let $O(V)$ be the orthogonal group of Q and $\Omega(V)$ the commutator group of $O(V)$. If the dimension n of V is $\geqq 3$ and the index ν of Q is $\geqq 1$, the factor group of $\Omega(V)$ modulo its center is simple except in the following cases:

(i) $n=3$ and k is the field of three elements; (ii) $n=4$ and $\nu=2$.

This theorem was proved by D. E. Dickson [3] in the case of finite ground field, then by J. Dieudonné [4] in the general case. In this paper we will give another proof of this theorem based on a principle given by K. Iwasawa in his paper [6]. The author wishes to express his hearty thanks to Professor Iwasawa who read the original manuscript and gave him several important suggestions.

For our convenience, we will use the same terminology as in C. Chevalley; *The algebraic theory of spinors,* Chapter I. We will define some notations we will use in this paper. The conjugate of a subspace U will be denoted by U'. If U is nonisotropic, the restriction Q_U of Q to U is a quadratic form whose associated bilinear form is nondegenerate. We will denote the index of Q_U (sometimes to be referred to as the index of U) by $\nu(U)$, the orthogonal group of Q_U by $O(U)$ and the commutator group of $O(U)$ by $\Omega(U)$. Since every $\rho_U \in O(U)$ is extended uniquely to $\rho \in O(V)$ which induces the identity transformation on U', we can consider $O(U)$ a subgroup of $O(V)$. The subspace spanned by vectors $x_1, \cdots, x_s$ will be denoted by $\langle x_1, \cdots, x_s \rangle$. If u is a nonsingular vector, we denote the symmetry with respect to the hyperplane $\langle u \rangle'$ by $\sigma_{\langle u \rangle}$. In the case of characteristic 2 the term "symmetry" means "transvection orthogonale" defined by J. Dieudonné [4], p. 41.

1. Subgroups $H_{\langle x \rangle}$.

LEMMA 1.[1] *Let x be a singular vector and u a vector in $\langle x \rangle'$. A linear*

---

* Received October 9, 1957.

[1] Orthogonal transformations of the type $\rho_{x,u}$ were introduced by M. Eichler in his

transformation $\rho_{x,u}$ *of* $\langle x\rangle'$ *defined by* $\rho_{x,u}(z) = z + B(z,u)x$ *is a* Q*-isomorphism of* $\langle x\rangle'$ *onto itself which leaves* x *fixed, and can be extended uniquely to an orthogonal transformation of* V.

Proof. It is clear that $\rho_{x,u}(x) = x$ and $\rho_{x,u}$ is a linear isomorphism of $\langle x\rangle'$ onto itself. Since $Q(u + cx) = Q(u)$ for every $u \in \langle x\rangle'$ and $c \in k$, it follows that $\rho_{x,u}$ is a Q-isomorphism. Let y be a singular vector such that $B(x,y) = 1$, and U the space $\langle x,y\rangle'$. Then we have $V = \langle x,y\rangle + U$ and $\langle x\rangle' = \langle x\rangle + U$.

For every $u \in \langle x\rangle'$ there exists a $u' \in U$ such that $u - u' \in \langle x\rangle$. It is clear that $\rho_{x,u} = \rho_{x,u'}$ because $B(z,u) = B(z,u')$ for every $z \in \langle x\rangle'$, so we may assume that $u \in U$. From Witt's theorem, there exists an extension $\rho \in O(V)$ of $\rho_{x,u}$. Put $\rho(y) = ax + by + v$ with $a, b \in k$ and $v \in U$. From the relations

$$B(\rho(x),\rho(y)) = B(x,y) = 1; \quad B(\rho(y),\rho(z)) = B(y,z) = 0 \text{ for all } z \in U,$$

and $Q(\rho(y)) = Q(y) = 0$, we have $b = 1$, $B(z,u) + B(z,v) = 0$ and $a + Q(V) = 0$. Then we have $\rho(y) = -Q(u)x + y - u$, hence ρ is uniquely determined.

We denote the extension ρ of $\rho_{x,u}$ by the same notation. The following properties of $\rho_{x,u}$ follow from the definition.

(i) $\rho_{x,u}\rho_{x,v} = \rho_{x,u+v}$ for $u, v \in \langle x\rangle'$.

(ii) $\rho_{x,cu} = \rho_{cx,u}$ for $0 \neq c \in k$.

(iii) $\tau\rho_{x,u}\tau^{-1} = \rho_{\tau(x),\tau(u)}$ for $\tau \in O(V)$.

(iv) $\rho_{x,u} = 1$ if and only if $u \in \langle x\rangle$.

It follows that the mapping $u \to \rho_{x,u}$ is an isomorphism of U into $O(V)$, and the image group depends only on the subspace $\langle x\rangle$. We will denote the subgroup by $H_{\langle x\rangle}$. From (iii), subgroups of this type are conjugate to each other. The minimum normal subgroup containing $H_{\langle x\rangle}$ will be denoted by $\Omega_1(V)$ (since $\Omega_1(V)$ is normal, the group contains all subgroups of the type $H_{\langle x\rangle}$, and is generated by those subgroups). The same notation will be used for nonisotropic subspaces U with $\dim U \geqq 3$ and $\nu(U) \geqq 1$.

---

proof of our fundamental theorem (cf. M. Eichler [5] (Chap. I, § 3). However, those transformations were already observed by C. L. Siegel to define the mass of representation of 0 by an indefinite quadratic form (cf. C. L. Siegel [7], p. 408).

Let $\bar{V}$ be the $n-1$ dimensional projective space whose points are 1-dimensional subspaces of V, and C the quadric in $\bar{V}$ defined by the equation $Q(x)=0$. For every subspace U of V we denote the intersection of C with $\bar{U}$ by C_U where $\bar{U}$ is the linear subvariety in $\bar{V}$ defined by U. If G is a group of linear transformations of V, we will denote the group of projective transformations induced by G by PG. For every nonsingular linear transformation τ of V, we denote by $\bar{\tau}$ the projective transformation induced by τ. If τ is an orthogonal transformation, then $\bar{\tau}$ maps C onto itself.

We will study the behavior of the group $P\Omega_1(V)$ as a transformation group of C.

LEMMA 2. *Let $p=\langle x\rangle$ be a point on C, and T_p the hyperplane defined by $\langle x\rangle'$, namely the tangential hyperplane of C at p. Let y be a singular vector such that $B(x,y)=1$, and U the conjugate of $\langle x,y\rangle$. Then the variety $K(p)=T_p\cap C$ is the projecting cone with the vertex p and a base variety C_U, and the group $\bar{H}_p=PH_{\langle x\rangle}$ is a simply transitive transformation group of the set $C-K(p)$.*

Proof. The first part is obvious because a vector z in $\langle x\rangle'$ is singular if and only if z is a linear combination of x and a singular vector v in U.

A point $\langle z\rangle$ on C is not on $K(p)$ if and only if $B(z,x)\neq 0$, so we can normalize z so that $B(x,z)=1$. Then the mapping $z\rightarrow\langle z\rangle$ is a one-to-one mapping of the set of all singular vectors z such that $B(x,z)=1$ onto the set $C-K(p)$. Put $z=ax+by+u$ with $a,b\in k$ and $u\in U$. From $B(x,z)=1$ and $Q(z)=0$, we have $b=1$ and $a=-Q(u)$, hence we have $z=\rho_{x,-u}(y)$. The mapping $u\rightarrow\langle\rho_{x,u}(y)\rangle$ is a one-to-one (birational) correspondence of U onto $C-K(p)$, and from $\rho_{x,u}(\rho_{x,v}(y))=\rho_{x,u+v}(y)$, we can see that $\bar{H}_p$ is a simply transitive transformation group of $C-K(p)$.

Remark. If $\nu=1$, $K(p)$ consists of only one point p.

LEMMA 3. *Let q and r be points on C; then there exists a point p on C such that both q and r do not lie on $K(p)$.*

Proof. Let y and z be singular vectors such that $q=\langle y\rangle$ and $r=\langle z\rangle$. At first we assume that $B(y,z)\neq 0$, so we may suppose that $B(y,z)=1$. Let u be a nonsingular vector in $\langle y,z\rangle'$. Put $x=\rho_{y,u}(z)=-Q(u)y+z-u$; then we have $B(x,y)=1$, $B(x,z)=-Q(u)$, hence q and r do not lie on $K(\langle x\rangle)$. Next, we assume that $B(y,z)=0$. Then the space $\langle y,z\rangle$ is totally singular, and it is well known that there exists a singular vector x such that $B(x,y)=B(x,z)=1$. Hence we have proved our assertion.

From Lemma 2 and Lemma 3, we have the following:

LEMMA 4. *The group* $P\Omega_1(V)$ *is a transitive transformation group of* C

LEMMA 5. *Let* p *be a point on* C *and* L_p *the group of all transformations in* $P\Omega_1(V)$ *which leave* p *fixed. If* $n \geqq 5$ *and* $\nu \geqq 2$, *the group* L_p *acts transitively on* $K(p) - p$.

Proof. Let x, y be a pair of singular vectors such that $p = \langle x \rangle$ and $B(x, y) = 1$. Let U be the subspace $\langle x, y \rangle'$. It is clear that the group H_p and the group $P\Omega_1(U)$ are contained in L_p. Since $K(p)$ is the projecting cone with the vertex p and a base variety C_U, every point on $K(p)$ lies on a line $p \cup s$ with $s \in C_U$. From the assumption, we have $\dim U \geqq 3$ and $\nu(U) \geqq 1$; hence, from Lemma 4, the group $P\Omega_1(U)$ acts transitively on C_U. Therefore if q and r are on $K(p) - p$, there exists a $\tau \in P\Omega_1(U)$ which maps q onto a point on the line $p \cup r$. Suppose that p, q and r are on the same line. Put $q = \langle y \rangle$ and $r = \langle z \rangle$. Then z is a linear combination $ax + by$ of x and y with $b \neq 0$. Let u be a vector in U such that $B(y, u) = a/b$. Then we have $\rho_{x,u}(y) = bz$ and $\bar{\rho}_{x,u}(q) = r$.

LEMMA 6. *Suppose that* $\nu \geqq 2$. *If* p *and* q *are distinct points on* C, *then there exists a point* $r \neq p$ *such that* $r \in K(p)$ *and* $r \notin K(q)$.

Proof. Put $p = \langle x \rangle$ and $q = \langle y \rangle$. If $\langle x, y \rangle$ is totally singular, then there exists a singular vector z such that $B(x, z) = 0$ and $B(y, z) = 1$. If $\langle x, y \rangle$ is nonisotropic, there exists a singular vector z' in $\langle x, y \rangle'$. Put $z = x + z'$. The point $r = \langle z \rangle$ satisfies our conditions in both cases.

LEMMA 7. *The group* $P\Omega_1(V)$ *is a primitive transformation group of* C *except in the case where* $n = 4$ *and* $\nu = 2$.

Proof. If $\nu = 1$, then from Lemma 2 and Lemma 4, the group $P\Omega_1(V)$ is 2-fold transitive, hence primitive. Suppose that $n \geqq 5$ and $\nu \geqq 2$. Let M be a subset of C with the following properties:

(i) M contains at least two points p and q.

(ii) For every $\tau \in P\Omega_1(V)$, such that $\tau M \cap M \neq \phi$, τM coincides with M.

We have only to show that M must be C itself. If the line $p \cup q$ lies on C, then from Lemma 5, both $K(p)$ and $K(q)$ are contained in M. From Lemma 6, there exists a point q' in $K(q)$ such that $q' \notin K(p)$. Hence we may assume that $p \cup q$ does not lie on C. Then from Lemma 2, we have $M \supset C - K(p)$, $C - K(q)$. From Lemma 6, there exists a point $r \in K(p)$ such that $r \neq p$ and $r \notin K(q)$. From Lemma 5, we have $K(p) \subset M$. Hence we have $M = C$.

2. The commutator group $\mathbf{\Omega}(V)$.

Lemma 8. *The group $\Omega_1(V)$ is a subgroup of $\Omega(V)$ except in the case where $k = F_2$, $n = 4$ and $\nu = 2$.*

Proof. Since $\Omega_1(V)$ is a normal subgroup of $O(V)$, we have only to prove that $H_{\langle x\rangle}$ is a subgroup of $\Omega(V)$, where x is a singular vector. Let y be a singular vector with $B(x,y) = 1$, and U the space $\langle x,y\rangle'$. If u is a nonsingular vector in U, we have

$$\begin{aligned} \sigma_{\langle u+Q(u)x\rangle}\sigma_{\langle u\rangle}(z) &= \sigma_{\langle u+Q(u)x\rangle}(z - B(u,z)u/Q(u)) \\ &= z - B(u,z)u/Q(u) - B(u+Q(u)x, z - B(u,z)u/Q(u))(u+Q(u)x)/Q(u) \\ &= z - B(u,z)u/Q(u) + B(u,z)(u+Q(u)x)/Q(u) = \rho_{x,u}(z) \end{aligned}$$

for every $z \in \langle x\rangle'$. From Lemma 1, we have $\rho_{x,u} = \sigma_{\langle u+Q(u)\rangle}\sigma_{\langle u\rangle}$. Since $Q(u) = Q(u + Q(u)x)$, there exists a $\tau \in O(V)$ which maps u onto $u + Q(u)x$. Therefore we have $\rho_{x,u} = \tau\sigma_{\langle u\rangle}\tau^{-1}\sigma_{\langle u\rangle} \in \Omega(V)$. Except in the case mentioned above, U is spanned by nonsingular vectors, so we have $H_{\langle x\rangle} \subset \Omega(V)$.

The following two lemmas are well known, so we omit the proof.

Lemma 9. *Except in the case excluded in Lemma 8, the commutator group of the proper orthogonal group*[2] *$O^+(V)$ is $\Omega(V)$.* (Cf. Chevalley [2], Chapter II. 3. 9.)

Lemma 10. *Except in the case excluded in Lemma* 8, *$\Omega(V)$ is generated by commutators of symmetries, and the order of every element in $O(V)/\Omega(V)$ is* 2. (Cf. Artin [1], Chapter IV, Theorem 3. 23.)

Now we will prove that $\Omega(V) = \Omega_1(V)$, except in a trivial case.

Lemma 11. *Let x and y be a pair of singular vectors such that $B(x,y) = 1$. Then we have $O(V) = O(\langle x,y\rangle)\Omega_1(V)$.*

Proof. Let u be a nonsingular vector. Then there exists a $u' \in \langle x,y\rangle$ such that $Q(u) = Q(u')$, hence there exists an orthogonal transformation τ such that $\tau(u') = u$. Put $\tau(x) = x'$ and $\tau(y) = y'$. From Lemma 2 and Lemma 4, there exists a $\tau' \in \Omega_1(V)$ such that $\tau'(\langle x\rangle) = \langle x'\rangle$, $\tau'(\langle y\rangle) = \langle y'\rangle$.

---

[2] In the case of characteristic 2, a proper orthogonal transformation is defined as a product of even number of symmetries.

Since $u \in \tau(\langle x, y\rangle) = \langle x', y'\rangle$, $u'' = \tau'^{-1}(u)$ is contained in $\langle x, y\rangle$. Hence we have

$$\sigma_{\langle u\rangle} = \tau'\sigma_{\langle u''\rangle}\tau'^{-1} = \sigma_{\langle u''\rangle}\,(\sigma_{\langle u''\rangle}{}^{-1}\tau'\sigma_{\langle u''\rangle}\tau'^{-1}) \in O(\langle x, y\rangle)\Omega_1(V).$$

Since $O(V)$ is generated by symmetries except in the case mentioned above, we have proved our assertion.

LEMMA 12. *Except in the case excluded in Lemma* 8, $\Omega_1(V)$ *coincides with* $\Omega(V)$.

Proof. It is obvious that $\Omega_1(V)$ is a subgroup of $O^+(V)$, hence, from Lemma 11, we have $O^+(V) = O^+(\langle x, y\rangle)\Omega_1(V)$ and

$$O^+(V)/\Omega_1(V) = O^+(\langle x, y\rangle)/O^+(\langle x, y\rangle) \cap \Omega_1(V).$$

Since $O^+(\langle x, y\rangle)$ is an abelian group, and from Lemma 9, we have $\Omega_1(V) \supset \Omega(V)$. Therefore from Lemma 8, we have $\Omega(V) = \Omega_1(V)$.

LEMMA 13. *The commutator group of* $\Omega(V)$ *coincides with* $\Omega(V)$ *except in the following two cases:*

(i) $n = 3$, $k = F_3$; (ii) $n = 4$, $\nu = 2$, $k = F_2$ or F_3.

Proof. At first we suppose that $k \neq F_2, F_3$. Then there exists a $c \in k$ such that $c^2 \neq 0, 1$. Let x, y be a pair of singular vectors with $B(x, y) = 1$, and τ the orthogonal transformation of $\langle x, y\rangle$ which maps x onto cx and y onto $c^{-1}y$. From Lemma 10, we have $\tau^2 \in \Omega(V)$ and

$$\tau^2\rho_{x,u}\tau^{-2}\rho_{x,u}{}^{-1} = \rho_{c^2x,u}\rho_{x,-u} = \rho_{x,(c^2-1)u} \qquad (u \in \langle x, y\rangle').$$

Since $c^2 - 1 \neq 0$, we have $H_{\langle x\rangle} \subset \Omega(V)'$, where $\Omega(V)'$ is the commutator group of $\Omega(V)$. From Lemma 12, we have $\Omega(V)' = \Omega(V)$.

Suppose that $k = F_2$ or F_3. Then we may assume that $n \geqq 5$ or $n = 4$ and $\nu = 1$. We have only to prove that $H_{\langle x\rangle} \subset \Omega(V)'$ as in the above treated case.

At first assume that $k = F_2$. Let u be a nonsingular vector in $\langle x, y\rangle'$. From the assumption, there exists a $v \in \langle x, y\rangle'$ such that $B(u, v) = Q(v) = 1$. Then the space $\langle u, v\rangle$ is nonisotropic and of index 0. Let τ be the orthogonal transformation of $\langle u, v\rangle$ such that $\tau(u) = v$, $\tau(v) = u + v$. Then we have $\tau^3 = 1$; hence, from Lemma 10, we have $\tau \in \Omega(V)$, and

$$\tau\rho_{x,v}\tau^{-1}\rho_{x,v}{}^{-1} = \rho_{x,u+v}\rho_{x,v}{}^{-1} = \rho_{x,u} \in \Omega(V)'.$$

Since $\langle x, y\rangle'$ is spanned by nonsingular vectors, we have $H_{\langle x\rangle} \subset \Omega(V)'$.

Next, we suppose $k = F_3$. Let u be a nonsingular vector in $\langle x, y\rangle'$, then from the assumption we can find a $v \in \langle x, y\rangle'$ such that $Q(u) = Q(v)$

and $B(u,v)=0$. Then the space $\langle u,v\rangle$ is nonisotropic and of index 0. Let τ be an element of $O(\langle u,v\rangle)$ such that $\tau(u)=-v$, $\tau(v)=u$. From Lemma 10, we have $\tau^2\in\Omega(V)$ and

$$\tau^2\rho_{x,u}\tau^{-2}\rho_{x,u}{}^{-1}=\rho_{x,-u}\rho_{x,-u}=\rho_{x,u}.$$

Hence we have $H_{\langle x\rangle}\subset\Omega(V)'$.

3. The proof of the fundamental theorem.

The following lemma is well known.

LEMMA 14. *The group $PO(V)$ is a faithful transformation group of C.* (Cf. J. Dieudonné [4], p. 30 and E. Artin [1], Theorem 3.18. The proofs given loc. cit. are valid in the case of characteristic 2 by slight modification.)

Now we can prove the simplicity of the group $P\Omega(V)$.

We exclude the following cases:

(i) $n=3$ and $k=F_3$; (ii) $n=4$ and $\nu=2$.

Let N be a normal subgroup of $P\Omega(V)$ and p a point on C. From Lemma 7, the subgroup L_p defined in Lemma 5 is maximal, and from Lemma 14, the intersection of all conjugate subgroups of L_p is $\{1\}$. It follows that if $N\neq\{1\}$, we have $NL_p=P\Omega(V)$, hence N is transitive on C. Therefore the group $N\bar{H}_p$ contains all conjugate subgroups of $\bar{H}_p$; hence, from Lemma 12, we have $N\bar{H}_p=P\Omega(V)$. Then we have $P\Omega(V)/N=\bar{H}_p/\bar{H}_p\cap N$. Since the group $\bar{H}_p$ is abelian, from Lemma 13 we have $N=P\Omega(V)$. Therefore the group $P\Omega(V)$ is simple.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] E. Artin, *Geometric algebra*, New York, Interscience, 1957.
[2] C. Chevalley, *The algebraic theory of spinors*, Columbia University Press, 1954.
[3] D. E. Dickson, *Linear groups*, Leipzig, B. C. Teubner, 1901.
[4] J. Dieudonné, *Sur les groupes classiques*, Actualités Scientifiques et Industrielles, No. 1040, 1948.
[5] M. Eichler, *Quadratische Formen und Orthogonale Gruppen*, Berlin, Springer, 1952.
[6] K. Iwasawa, "Über die Einfachheit der speziellen projectiven Gruppen," *Proceedings of the Imperial Academy of Tokyo*, vol. 17 (1941), pp. 57-59.
[7] C. L. Siegel, "Über die Zetafunktionen indefiniter Quadratischer Formen. II," *Mathematische Zeitschrift*, vol. 44 (1938), pp. 398-426.

ON THE ANALYTICITY OF THE SOLUTIONS OF ANALYTIC NON-LINEAR ELLIPTIC SYSTEMS OF PARTIAL DIFFERENTIAL EQUATIONS.*[1]

By CHARLES B. MORREY, JR.

PART I. Analyticity in the Interior.

1. Introduction. In this part, we prove that any solution $u = (u^1, \cdots, u^N)$ in which each u^k is of class $C^{t_k+\mu}$, $0 < \mu < 1$, (for notations, etc., see below) of a non-linear analytic elliptic system

$$\phi_j(x, \cdots, u^k, \nabla u^k, \cdots, \nabla^{s_j+t_k} u^k, \cdots) = 0, \qquad j = 1, \cdots, N \qquad (x = (x^1, \cdots, x^\nu)) \tag{1.1}$$

of the type considered by Nirenberg and Douglis ([3], p. 532) is analytic at each interior point of its domain. The analyticity at the boundary for non-linear strongly-elliptic systems [11] will be considered in Part II.

The analyticity of any solution $u(x, y)$ of class C''' of a single non-linear analytic elliptic equation with $\nu = 2$ was first proved in a famous memoir of S. Bernstein [1] in 1904. Other proofs of Bernstein's theorem were given by M. Gevrey [5], T. Radó [13] and H. Lewy [8] and by Bernstein himself [2]. E. Hopf [6] proved the corresponding theorem for a single equation but with any value of ν. Finally, Petrowsky [12] proved the theorem for systems which are almost as general as those considered here. Very recently, the analyticity of the solutions of *linear* elliptic systems in the interior and at the boundary has been proved by Morrey and Nirenberg [10]. Still more recently, after this paper had appeared as a report, Avner Friedman [4] extended these results and those of Part II to obtain corresponding results for quasi-analytic systems and more general systems in which the ϕ_j belong to the M_n classes of Mandebrojt [9]. His methods are entirely different from those in this paper and involve mainly bounds for the derivatives as in [10] and [5].

The proofs of Lewy, Hopf, and Petrowsky all involved extension to the

---

* Received September 30, 1957.

[1] The research reported in this paper was partially supported by contract Nonr-222(37) with the Office of Naval Research.

complex domain. Lewy used his theory of hyperbolic equations to carry out the extension and Hopf's method involved the extension of certain generalized potentials to the complex domain, an idea which had been used by E. E. Levi [7]. The present paper combines this idea with a simple type of implicit function theorem in a Banach space to yield a proof which is a great deal simpler than that of Petrowsky and somewhat simpler (for the interior) than the preceding proofs except for that of Lewy and the second proof of Bernstein [2]. Of the writers mentioned above, only Morrey and Nirenberg [10], Avner Friedman [4], and Gevrey [5], considered analyticity at the boundary.

In the systems (1.1) which we consider in this paper, it is assumed that there are integers $s_1, \cdots, s_N$ and $t_1, \cdots, t_N$ such that only derivatives of order $\leqq s_j + t_k$ of u^k occur in ϕ_j. Furthermore, we assume (with Douglis and Nirenberg) that only *derivatives* of order $\geqq 0$ occur. Since we may add the same integer to all the t_j and subtract it from all the s_j, we assume (as in [3]) that

$$(1.2) \qquad \max_{1 \leqq j \leqq N} s_j = 0.$$

As in [3], we say that the system (1.1) is *elliptic along a vector* $u_0(x)$ if and only if the equations of variation

$$(1.3) \qquad \begin{aligned} &L_{jk}(x, D) v^k \\ &\equiv \frac{d}{d\lambda} \phi_j[x, \cdots, u^k + \lambda v^k, \cdots, \nabla^{s_j + t_k}(u^k + \lambda v^k), \cdots] \,|_{\lambda=0} = 0 \end{aligned}$$

form a linear elliptic system of the type in [3]. If $L^0{}_{jk}(x, D)$ denotes the terms of $L_{jk}(x, D)$ of order *exactly* $s_j + t_k$ ($\equiv 0$ if $s_j + t_k < 0$), the system (1.3) is said to be elliptic if and only if the determinant

$$(1.4) \qquad L(x, \lambda) \equiv | L^0{}_{jk}(x, \lambda) | \neq 0 \text{ for real } \lambda \neq 0,$$

$L^0{}_{jk}(x, \lambda)$ being the characteristic polynomial of the operator $L^0{}_{jk}(x, D)$. It is to be noticed that this determinant is a homogeneous polynomial in λ of degree

$$(1.5) \qquad m = \sum_{j=1}^{N} (s_j + t_j) \geqq 0.$$

The functions ϕ_j, u^k, and the coefficients in the L_{jk} may be complex-valued.

We use the following notations: Repeated indices are summed unless otherwise noted. If ϕ is a vector or tensor with either real or complex-valued components, $|\phi|$ denotes the square root of the sum of the squares of the components and $\|\phi\|$ denotes the square root of the sum of the squares of the absolute values of the components; the absolute value of a single complex number z is denoted by $|z|$. The double bars will also denote norms in certain spaces to be introduced. A tensor will be of class $C^{n+\mu}$, $0<\mu<1$, in a closed domain $\bar{D}$ in real or complex space if and only if each component is of class C^n on D and each of its n-th derivatives satisfies a uniform Hölder condition with exponent μ on D (and so can be extended to $\bar{D}$, etc.). If the tensor u is of class C^μ on D, D being in the real space, we define

$$h_\mu(u)=\sup|x_2-x_1|^{-\mu}\|u(x_2)-u(x_1)\| \text{ for all } x_1,x_2 \text{ on } D \text{ with } x_1\neq x_2;$$

$h^*_\mu(u)$ is defined correspondingly if D is in complex space. If u^k is a vector, $\nabla^p u^k$ denotes the tensor $u^k{}_{,\alpha_1\cdots\alpha_p}$, the subscripts after the comma denoting patrial differentiation with respect to $x^{\alpha_1}\cdots x^{\alpha_p}$; the definition extends to tensors u. $B(x_0,R)$ denotes the ball $|x-x_0|<R$ in real ν-space and $B_R=B(0,R)$. B_{hR} denotes the set of all complex vectors $x=(x^1,\cdots,x^\nu)=x_1+ix_2$ in which

$$B_{hR}\colon\ |x_1|<R,\ |x_2|<h(R-|x_1|).$$

If condition (1.4) holds for all x on a closed domain $\bar{D}$ and $L(x,\lambda)$ is continuous it follows that

$$m_1>0, \text{ where } m_1=\min|L(x,\lambda)| \text{ for } x\in\bar{D},\ |\lambda|=1.$$

We let M denote a bound for the coefficients occurring in any of the L_{jk} operators used. The constants K_1,K_2,K_{3q}, etc., and $Z_1,Z_2,\cdots$ will depend only on the numbers $\nu,N,s_1,\cdots,s_N$, $t_1,\cdots,t_N,m_1$, and M unless the numbers μ and h enter in which case we shall write $K_1(\mu,h)$, etc. The K's are permanent constants whereas the Z's are used only in the course of a single proof, so that Z_1 may denote different constants in different proofs.

We now outline our method of proof. Suppose we have a solution of (1.1) in which each u^k is of class $C^{t_k+\mu}$, $0<\mu<1$, near some point x_0. By a translation of axes, we may assume $x_0=0$. Next, let $P^k(x)$ be that polynomial of degree t_k such that

$$\nabla^p P^k(0)=\nabla^p u^k(0), \qquad 0\leqq p\leqq t_k. \tag{1.6}$$

Making the substitution

$$u^k=P^k+v^k \tag{1.7}$$

in (1.1) we obtain new equations of the same type in which $\nabla^p v^k(0)=0$

for $0 \leqq p \leqq t_k$. If we expand the new ϕ_j about the origin we may rewrite the new equations in the form

$$L_{jk}v^k = M_{jk}v^k + \psi_j(x, \cdots, v^k, \cdots, \nabla^{s_j+t_k}v^k, \cdots) \tag{1.8}$$

where now the $L_{jk}(D)$ are operators with constant coefficients containing the derivatives or order exactly $s_j + t_k$, the $M_{jk}(D)$ are operators with constant coefficients of order $< s_j + t_k$, and ψ_j is the remainder term. Since L_{jk} contains derivatives of v^k of order $s_j + t_k$ and $s_j \leqq 0$, we may differentiate (1.8) $(-s_j)$ times with respect to the x^α. Since all derivatives of v^k up to the order t_k vanish at the origin, we note that the Taylor expansion of ψ_j begins with a homogeneous polynomial in x of degree $1 - s_j$, linear terms in the $\nabla^p v^k$ with coefficients homogenous and linear in x, and quadratic terms in the $\nabla^p v^k$ with constant coefficients.

In Sections 2 and 3 we prove the following theorem:

THEOREM A. *For each $R > 0$, there exists a linear transformation $u = P_R(f)$ from the space of vectors f in which f_j is of class $C^{\mu-s_j}$, $0 < \mu < 1$, on $\bar{B}_R$ with $\nabla^p f_j(0) = 0$ for $0 \leqq p \leqq -s_j$ into the space of vectors u in which u^k is of class $C^{t_k+\mu}$ on $\bar{B}_R$ with $\nabla^p u^k(0) = 0$, $0 \leqq p \leqq t_k$ such that*

$$L_{jk}u^k = f_j \tag{1.9}$$

in which L_{jk} is an operator of the type in (1.8). Moreover,

$$\max_{1 \leqq k \leqq N} h_\mu(\nabla^{t_k}u^k) \leqq K_1(\mu) \max_{1 \leqq j \leqq N} h_\mu(\nabla^{-s_j}f_j). \tag{1.10}$$

In the space of vectors u described in this theorem, we introduce the norm

$$\| u \| = \max_{1 \leqq k \leqq N} h_\mu(\nabla^{t_k}u^k) \qquad (x \text{ on } \bar{B}_R). \tag{1.11}$$

The resulting space is clearly a Banach space which we denote by E_R. Clearly, if $u \in E_R$, we see that

$$\begin{gathered} \| \nabla^{t_k}u^k(x) \| \leqq \| u \| \cdot | x |^\mu, \\ \| \nabla^p u^k(x) \| \leqq \| u \| \cdot | x |^{t_k-p+\mu}/(1+\mu) \cdots (t_k - p + \mu), \\ 0 \leqq p < t_k. \end{gathered} \tag{1.12}$$

We wish to replace (1.8) by an equation involving operators on E_R. To do this we write

$$v = V_R + H_R, \qquad V_R = P_R(f), \tag{1.13}$$

where f denotes the right side of (1.8). If v is given, as is assumed, V_R is known and H_R is known. Moreover, H_R is a solution of the homogeneous equation (1.9) with $f=0$. We shall regard H_R as known and try to find an equation for V_R. To do this we substitute (1.13) into the right side of (1.8) and define

$$\begin{aligned} W_R &= P_R\{M_{jk}H_R^k + \psi_j(x, \cdots, H_R, \cdots)\}, \\ T_R(V_R; H_R) &= P_R\{M_{jk}V_R^k + \psi_j(x, \cdots, H_R + V_R, \cdots) - \psi_j(x, \cdots, H_R, \cdots)\} \end{aligned} \tag{1.14}$$

Then (1.8) is equivalent to the operator equation

$$V_R - T_R(V_R; H_R) = W_R, \tag{1.15}$$

where W_R is, of course, known if H_R is.

Now, of course, $\| v \| \leqq M_1$ independently of R for our solution and so $\| H_R \| \leqq M_2$ for all $R \leqq R_0$, say. From (1.12), we see that if we restrict ourselves to elements H_R and V_R with norms $\leqq M_2$, then W_R and $T_R(V_R, H_R)$ are defined for sufficiently small R. By using (1.12), (1.14), the form of ψ_j, and that of the M_{jk} (operator of lower order than L_{jk}), it is straightforward to verify that

$$\begin{aligned} &T_R(0; H_R) = 0, \quad \| T_R(V_{1R}; H_R) - T_R(V_{2R}; H_R) \| \leqq \epsilon_1(R) \cdot \| V_{1R} - V_{2R} \| \\ &\| W_R \| \leqq \epsilon_2(R), \quad \lim_{R \to 0} \epsilon_i(R) = 0, \; \| H_R \|, \| V_{1R} \|, \| V_{2R} \| \leqq M_2. \end{aligned} \tag{1.16}$$

Thus if $R \leqq R_1$, *say, there is a unique solution* V_R *of* (1.15) *for which* $\| V_R \| \leqq M_2$ *for any given* H_R *with* $\| H_R \| \leqq M_2$.

For given numbers $R > 0$ and h, $0 < h < 1$, let us introduce the space E^*_{hR} of vectors u in which u^k is analytic in B_{hR}, u^k is of class $C^{t_k+\mu}$ on $\bar{B}_{hR}$, and $\nabla^p u^k(0) = 0$ for $0 \leqq p \leqq t_k$ in which we define $\| u \|^*$ by (1.11) with h_μ replaced by h^*_μ. We introduce the corresponding space F^*_{hR} of vectors f. Obviously, if $u \in E^*_{hR}$ for some $h > 0$, $u \in E_R$ and $\| u \|^* \geqq \| u \|$. In Section 4, the following two theorems are proved:

THEOREM B. *There is a number* $h_0 = h_0(\mu, \nu, N, s_j, t_j, m_1, M) > 0$ *such that if* $f \in F^*_{hR}$ *with* $0 < h \leqq h_0$ *and* $u = P_R(f)$, *then* u *can be extended to* $\bar{B}_{hR}$ *so that* $u \in E^*_{hR}$ *and*

$$\| u \|^* \leqq K_2(h, \mu) \max_{1 \leqq j \leqq N} h^*_\mu(\nabla^{-s_j} f_j). \tag{1.17}$$

THEOREM C. *If $H_R \in E_R$, then H_R can be extended analytically to any B_{hR} with $0 < h \leqq h_0$ and the extended function $\in E^*_{hR}$ with*

$$\| H_R \|^* \leqq K_3(h, \mu) \| H_R \|. \tag{1.18}$$

From Theorem B, it follows that *the operator $T_R(V_R, H_R)$ can be defined for functions V_R and H_R in any B_{hR} with $0 < h \leqq h_0$ and $0 < R \leqq R_2$ and, moreover, that* (1.16) *holds with the norm $\| \phi \|$ replaced by $\| \phi \|^*$* (and different functions $\epsilon_i(R)$).

Now, let us revert to our given solution v, and let V_R and H_R be defined as before. From Theorem C, we see that $\| H_R \|^* \leqq M_3$ for $0 < R \leqq R_3$. From the underlined results, we see that *if R is small enough, there are unique solutions V_R and $\tilde{V}_{h_0R}$ in E_R and $E^*_{h_0R}$ respectively, of* (1.15) *with $\| V_R \| \leqq M_2$ and $\| \tilde{V}_{h_0R} \| \leqq M_3$ for our given H_R. Since $E^*_{h_0R} \subset E_R$, $\tilde{V}_{h_0R} = V_R$ so V_R and hence v are analytic; in fact they can be extended analytically to B_{h_0R} and their extensions $\in E^*_{h_0R}$.*

2. The particular solutions. In this section, we construct the particular solutions of equations (1.9) which were mentioned in the introduction and prove Theorem A. For the moment, we shall merely asume that the f_j are of class $C^{\mu - s_j}$ $(0 < \mu < 1)$ and shall drop the requirements that $\nabla^p f_j(0) = 0$ for $0 \leqq p \leqq -s_j$. These developments are very similar to those of Nirenberg and Douglis [3].

We define

$$G_{1n}(u) = (u^n/n!)(\log |u| - C_n), \tag{2.1}$$
$$C_n = 1 + 1/2 + \cdots + 1/n, \qquad G_{2n}(u) = u^n |u| / (n+1)!.$$

Then

$$G^{(k)}{}_{jn}(u) = G_{j,n-k}(u), \qquad 0 \leqq k \leqq n, j = 1, 2. \tag{2.2}$$

Next, if $m > 0$, we define

$$J^*(y) = \begin{cases} C_{1\nu} \displaystyle\int_{|\lambda|=1} G_{1m}(y \cdot \lambda) L^{-1}(\lambda) d\Sigma_\lambda, & \nu \text{ even}, \\ C_{2\nu} \displaystyle\int_{|\lambda|=1} G_{2m}(y \cdot \lambda) L^{-1}(\lambda) d\Sigma_\lambda, & \nu \text{ odd}, \end{cases} \tag{2.3}$$

$$J(y) = \begin{cases} \Delta^{\nu/2} J^*(y), & \nu \text{ even}, \\ \Delta^{(\nu+1)/2} J^*(y), & \nu \text{ odd}. \end{cases} \tag{2.4}$$

Let L be the scalar operator having $L(\lambda)$ as characteristic polynomial. Then

$$(2.5)\qquad LJ^*(y)=M_\nu(y)=\begin{cases} C_{1\nu}\displaystyle\int_{|\lambda|=1} G_{10}(y\cdot\lambda)\,d\Sigma_\lambda, & \nu \text{ even},\\ C_{2\nu}\displaystyle\int_{|\lambda|=1} G_{20}(y\cdot\lambda)\,d\Sigma_\lambda, & \nu \text{ odd}.\end{cases}$$

Clearly J is homogeneous of degree $m-\nu$ unless ν is even and $m-\nu\geqq 0$ in which case

$$(2.6)\qquad J(y)=J_1(y)\log|y|+J_2(y),$$

where J_1 is a *polynomial* and J_1 and J_2 are homogeneous of degree $m-\nu$; and

$$(2.7)\qquad J(-y)=(-1)^m J(y).$$

Finally, for each j and a given $R>0$, we define

$$(2.8)\qquad F_j(x)=\int_{B_R} J(x-\xi)f_j(\xi)\,d\xi,\quad F^*_j(x)=\int_{B_R} J^*(x-\xi)f_j(\xi)\,d\xi.$$

The constants $C_{1\nu}$ and $C_{2\nu}$ are chosen so that

$$(2.9)\qquad \Delta^{-1+\nu/2}M(y)=\Gamma_0(y),\ \text{if } \nu \text{ even},\quad \Delta^{-1+(\nu+1)/2}M(y)=\Gamma_0(y)\ \text{if } \nu \text{ odd},$$
$$\Gamma_0(y)=-(\nu-2)^{-1}|\Sigma|^{-1}\cdot|y|^{2-\nu},\ \nu>2,\ \Gamma_0=\tfrac{1}{2\pi}\log|y|,\ \nu=2$$

where $|\Sigma|$ is the $(\nu-1)$-measure of $\partial B(0,1)$; Γ_0 is just the elementary function for Laplace's equation.

It follows from (2.1)-(2.9) that

$$(2.10)\qquad LF^*_j(x)=\int_{B_R} M(x-\xi)f_j(\xi)\,d\xi.$$

From the form of M, it follows that we may differentiate the right side of (2.10) $(\nu-1)$ times under the integral sign. Thus from (2.9) and ordinary potential theory we see that

$$(2.11)\qquad \begin{cases}\Delta^{\nu/2}LF^*_j(x)=f_j(x), & \nu \text{ even},\\ \Delta^{(\nu+1)/2}LF^*_j(x)=f_j(x), & \nu \text{ odd}.\end{cases}$$

In the next section, we shall see that each F_j is of class $C^{m-s_j+\mu}$ on $\bar B_R$ and that

$$(2.12)\qquad h_\mu(\nabla^{m-s_j}F_j)\leqq K_0\cdot h_\mu(\nabla^{-s_j}f_j),\quad K_0=K_0(\mu,\nu,N,m_1,M).$$

As soon as that is shown, it will follow that

$$(2.13)\qquad LF_j(x)=f_j(x),\quad x\in B_R\ (\bar B_R \text{ by continuity}).$$

In case $m=0$, then $L(\lambda)$ is just a constant, L is a constant operator, we define $F_j(x) = L^{-1}f_j(x)$, and (2.13) holds, of course, and the differentiability properties of F_j hold.

Let us grant the statements above about the F_j. Let

$$\| L^{pj}(\lambda) \| = \| L_{jk}(\lambda) \|^{-1} \cdot L(\lambda) \tag{2.14}$$

and let $L^{pj}(D)$ be the corresponding operators; $L^{pj}(D) \equiv 0$ or is an operator of order $m - s_j - t_j \geqq 0$. Let us define

$$U^p(x) = L^{pj}F_j(x) \tag{2.15}$$

Then from (2.12) and (2.15), we see that U^p is of class $C^{t_p+\mu}$ on $\bar{B}_R$ so that

$$L_{jk}U^k(x) = L_{jk}L^{kl}F_l(x) = \delta^l{}_j LF_l(x) = LF_j(x) = f_j(x). \tag{2.16}$$

Finally, suppose

$$\nabla^p f_j(0) = 0, \qquad 0 \leqq p \leqq -s_l. \tag{2.17}$$

Let U be the solution (2.15) and let Q^k be the polynomial of degree t_k such that (2.18) holds, and define u^k by (2.18):

$$\nabla^p Q^k(0) = \nabla^p U^k(0), \ 0 \leqq p \leqq t_k, \ u^k(x) = U^k(x) - Q^k(x). \tag{2.18}$$

Then

$$L_{jk}u^k(x) = f_j(x) - q_j(x), \qquad j = 1, \cdots, N, \tag{2.19}$$

where q_j is a polynomial of degree $-s_j$. Differentiating (2.19) p times and setting $x = 0$, $p = 0, 1, \cdots, -s_j$, we see that $q_j(x) \equiv 0$. Thus Theorem A will be completely proved as soon as the differentiability properties of F_j are proved.

3. The analyticity of J and J^*; the differentiability of the F_j. We first prove the analyticity of J and J^*. To this end, we prove:

LEMMA 3.1. *Suppose y_0 is a real vector and $y_0 \neq 0$. Then there is a linear transformation*

$$\lambda_\alpha = \lambda_\alpha(\mu, y) \equiv h_\alpha{}^\beta(y)\mu_\beta \tag{3.1}$$

which is orthogonal for each real y near y_0, in which the $h_\alpha{}^\beta(y)$ are analytic and positively homogeneous of degree 0 for all complex y near y_0, and for which

$$\lambda_\alpha y^\alpha = \mu_1 \, | y |, \text{ where } | y | = [\sum_{\alpha=1}^{\nu} (y^\alpha)^2]^{\frac{1}{2}}. \tag{3.2}$$

Proof. Using a fixed orthogonal transformation, we easily reduce the problem to the case where

$$y_0{}^{\alpha} = |y_0| \delta^{\alpha}{}_1. \tag{3.3}$$

Since we may solve (3.1) for μ, obtaining $\mu_\alpha = h_\beta{}^\alpha \lambda_\beta$ we see that (3.2) implies that $h_\alpha{}^1(y) = y^\alpha/|y|$. It is easy to see that there is a unique way to complete the matrix h to be orthogonal with all the minors in the upper left hand corner positive, and with $h_\alpha{}^\beta(y) = 0$ for $\alpha > \beta$; this is all for real y sufficiently near y_0. The $h_\alpha{}^\beta$ are analytic for complex y near y_0.

LEMMA 3.2. *$J^*(y)$ and $J(y)$ are analytic for all real $y \neq 0$.*

Proof. Suppose y_0 is real and $y_0 \neq 0$. From (2.3) we have

$$\begin{aligned} J^*(y) &= C_{1\nu} \int_{|\lambda|=1} G_m(\lambda \cdot y) L^{-1}(\lambda)\, d\Sigma_\lambda = J_1{}^*(y) \log |y| \\ &\quad + C_{1\nu} |y|^m \int_{|\mu|=1} ((\mu^1)^m/m!) [\log |\mu^1| - C_m] L^{-1}[\lambda(\mu, y)]\, d\Sigma_\mu \end{aligned} \tag{3.4}$$

for all real y near y_0 if ν is even, $J_1{}^*$ being a polynomial of degree m. The analyticity of J^* follows in this case from (3.4) and that of J follows from (2.4). The proof for ν odd is similar.

ASSUMPTION. *We assume hereafter that $m > 0$ since the differentiability properties of the F_j are proved in the case $m = 0$.*

LEMMA 3.3. *The functions F_j of (2.8) are of class $C^{m+\mu-s_j-1}$ on $\bar{B}_R$ and each component of $\nabla^{m-s_j-1} F_j$ is of the form*

$$\begin{aligned} F_{j,\alpha_1 \cdots \alpha_{m-1} \beta_1 \cdots \beta_n}(x) &= -\int_{\partial B_R} \Gamma_{,\beta_2 \cdots \beta_n}(x-\xi) f_j(\xi)\, d\xi'_{\beta_1} \\ &- \int_{\partial B_R} \Gamma_{,\beta_3 \cdots \beta_n}(x-\xi) f_{j,\beta_1}(\xi)\, d\xi'_{\beta_2} - \cdots - \int_{\partial B_R} \Gamma(x-\xi) f_{j,\beta_1 \cdots \beta_{n-1}}(\xi)\, d\xi'_{\beta_n} \\ &+ \int_{B_R} \Gamma(x-\xi) f_{j,\beta_1 \cdots \beta_n}(\xi)\, d\xi, \quad n = -s_j; \end{aligned} \tag{3.5}$$

$$\Gamma(y) = J_{,\alpha_1 \cdots \alpha_{m-1}}(y); \tag{3.6}$$

the function Γ is homogeneous of degree $1-\nu$, analytic for $y \neq 0$, and

$$\Gamma(-y) = -\Gamma(y) \tag{3.7}$$

Proof. If $-s_j = n \geqq 1$, we see that

$$F_{j,\beta_1}(x) = \int_{B_R} J_{,\beta_1}(x-\xi) f_j(\xi)\, d\xi = -\int_{B_R} [\partial J(x-\xi)/\partial\xi^{\beta_1}] f_j(\xi)\, d\xi$$
$$= -\int_{\partial B_R} J(x-\xi) f_j(\xi)\, d\xi'_{\beta_1} + \int_{B_R} J(x-\xi) f_{j,\beta_1}(\xi)\, d\xi.$$

The form (3.5) follows by repeating this argument and then differentiating with respect to $x^{\alpha_1}, \cdots, x^{\alpha_{m-1}}$. That Γ is analytic for $y \neq 0$ and satisfies (3.7) follows from (3.6), Lemma 3.2, and (2.7).

From Lemma 3.3, it follows that the desired differentiability results for the F_j will be proved if we can show that if

$$U(x) = \int_{B_R} \Gamma(x-\xi) f(\xi)\, d\xi, \quad f \in C^{0+\mu} \text{ on } \bar{B}_R, \tag{3.8}$$

$$W_\gamma(x) = -\int_{\partial B_R} \Gamma(x-\xi) f(\xi)\, d\xi'_\gamma \quad f \in C^{q+\mu} \text{ on } \bar{B}_R,\ q \geqq 0, \tag{3.9}$$

then U is of class $C^{1+\mu}$ on $\bar{B}_R$ and W is of class $C^{q+\mu}$ on $\bar{B}_R$, and

$$h_\mu(\nabla U) \leqq K_4(\mu) h_\mu(f), \qquad h_\mu(\nabla^q W) \leqq K_{5q}(\mu) h_\mu(\nabla^{q+1} f) \tag{3.10}$$

ASSUMPTION. *In all the following lemmas,* Γ *is assumed to have the properties given in Lemma* 3.3.

To prove the statements above, we first prove the following well-known lemma which is hard to find in the literature (but cf. [6]).

LEMMA 3.4. *Suppose* Γ *satisfies the conditions of Lemma* 3.3. *Then*

$$\int_{\partial B(x_0,R)} \Gamma(\xi - x)\, d\xi'_\gamma = \int_{\partial B(0,1)} \Gamma(\eta)\, d\eta'_\gamma \equiv \int_{\partial B(0,1)} \Gamma(\eta) \eta^\gamma\, dS_\eta, \quad x \in B(x_0, R). \tag{3.11}$$

Proof. If $x = x_0$, the result is obvious from the homogeneity. If $x \in B(x_0, R)$ but $x \neq x_0$, and if $|\eta| = 1$, we define ξ and λ by

$$\begin{gathered} \xi - x_0 = (x - x_0) + \lambda\eta, \quad R^2 = r^2 + 2\lambda r(\omega \cdot \eta) + \lambda^2, \\ \omega = (x - x_0)/|x - x_0|, \quad r = |x - x_0|, \\ \lambda = -r\cos\psi + (R^2 - r^2 \sin^2\psi)^{\frac{1}{2}}, \cos\psi = \omega \cdot \eta. \end{gathered} \tag{3.12}$$

Then

$$|\xi - x| = \lambda, \quad d\xi'_\gamma = [(\xi^\gamma - x_0{}^\gamma)/R]\, dS_\xi = [(\xi^\gamma - x_0{}^\gamma)/R] \cdot \lambda^{\nu-1} \sec X\, dS_\eta, \tag{3.13}$$

where X is the angle between the vectors $\overrightarrow{x\xi}$ and $\overrightarrow{x_0\xi}$, and

$$\sec X = 2R\lambda/(R^2 + \lambda^2 - r^2) = R/(R^2 - r^2 \sin^2\psi)^{\frac{1}{2}} \tag{3.14}$$

from (3.12). Substituting (3.13) and (3.14) in (3.11) and using the properties of Γ, we obtain

$$\int_{\partial B(x_0,R)} \Gamma(\xi - x)\, d\xi'_\gamma = \int_{\partial B(0,1)} \Gamma(\eta) \cdot (\xi^\gamma - x_0{}^\gamma)/R \cdot R/(R^2 - r^2 \sin^2 \psi)^{\frac{1}{2}} dS_\eta$$

$$= \int_{\partial B(0,1)} \Gamma(\eta)\eta^\gamma \, dS_\eta$$

$$+ \int_{\partial B(0,1)} \Gamma(\eta) \cdot [(x^\gamma - x_0{}^\gamma) + r(\omega \cdot \eta)\eta^\gamma]/(R^2 - r^2 \sin^2 \psi)^{\frac{1}{2}} \, dS_\eta$$

and the last integral is zero on account of (3.7).

As an immediate consequence of Lemma 3.4, we obtain

LEMMA 3.5. *There are constants* $C^{\beta_1 \cdots \beta_n}_{\alpha_1 \cdots \alpha_n \gamma}$ *which depend on* Γ *but whose magnitudes depend only on* $\nu, N, s_j, t_j, m_1,$ *and* M *such that*

$$-\int_{\partial B(x_0,R)} \Gamma_{,\alpha_1 \cdots \alpha_n}(x - \xi) \cdot (\xi^{\beta_1} - x^{\beta_1}) \cdots (\xi^{\beta_n} - x^{\beta_n})\, d\xi'_\gamma$$

$$= C^{\beta_1 \cdots \beta_n}_{\alpha_1 \cdots \alpha_n \gamma}, \quad x \in B(x_0, R),$$

$$-\int_{\partial B(x_0,R)} \Gamma_{,\alpha_1 \cdots \alpha_n}(x - \xi) \cdot (\xi^{\beta_1} - x^{\beta_1}) \cdots (\xi^{\beta_p} - x^{\beta_p})\, d\xi'_\gamma = 0, \quad p < n,$$

$$x \in B(x_0, R),$$

$$\int_{\partial B(x_0,R) - B(x_1,\rho)} \Gamma_{,\alpha_1 \cdots \alpha_n}(x - \xi) \cdot (\xi^{\beta_1} - x^{\beta_1}) \cdots (\xi^{\beta_p} - x^{\beta_p})\, d\xi = 0, \quad p < n,$$

$$x \in B(x_1, \rho) \subset B(x_0, R).$$

LEMMA 3.6. *Suppose* W_γ *is given by* (3.9), *where* $f \in C^{q+\mu}$ *on* $\bar{B}_R$. *Then* $W \in C^{q+\mu}$ *on* $\bar{B}_R$ *and* $h_\mu(\nabla^q W_\gamma) \leqq K_{5q}(\mu) h_\mu(\nabla^q f)$.

Proof. Differentiating (3.9), $q+1$ times and using Lemma 3.5, we obtain

$$(3.15) \quad \nabla^{q+1} W = -\int_{\partial B_R} \nabla^{q+1}\Gamma(x - \xi)[f(\xi) - \sum_{j=0}^{q} \nabla^j f(x) \cdot (\xi - x)^j / j!]\, d\xi'_\gamma, \quad x \in B,$$

where the sum in the bracket denotes the Taylor expansion of f out to the terms of order q. Taking magnitudes, we obtain

$$|\nabla^{q+1} W_\gamma(x)| \leqq \Gamma_{q+1} \cdot h_\mu(\nabla^q f) \int'_{\partial B_R} |x - \xi|^{\mu-\nu} dS_\xi \leqq Z_1(\mu) h_\mu(\nabla^q f) \cdot (R - |x|)^{\mu-1}.$$

Since any two points in B_R can be joined by an arc $x = x(s)$, $0 \leqq s \leqq l$ (s arc length) such that

$$\int_0^l (R - |x(s)|)^{\mu-1} ds \leqq 3\mu^{-1} |x_1 - x_2|^\mu,$$

the result follows.

LEMMA 3.7. *Suppose U is given by (3.8), where $f \in C^{\mu}$ on $\bar{B}_R$. Then U is of class $C^{1+\mu}$ on B_R and*

$$U_{,\alpha}(x) = C_\alpha f(x) + \int_{B_R} \Gamma_\alpha(x-\xi)[f(\xi)-f(x)]\,d\xi \tag{3.16}$$

$$x \in B_R,\ C_\alpha = -\int_{\partial B_R} \Gamma(y)\,dy'_\alpha.$$

Moreover, $h_\mu(\nabla U) \leqq K_4(\mu) h_\mu(f)$.

Proof. Let us extend f to be of class C^{μ} on $\bar{B}_{2R}$ with the same Hölder condition. Then

$$U = U_1 - U_2, \qquad U_1(x) = \int_{B_{2R}} \Gamma(x-\xi) f(\xi)\,d\xi, \tag{3.17}$$

$$U_2 = \int_{B_{2R}-B_R} \Gamma(x-\xi) f(\xi)\,d\xi.$$

We have

$$U_{2,\alpha}(x) = \int_{B_{2R}-B_R} \Gamma_{,\alpha}(x-\xi) f(\xi)\,d\xi$$

$$= \int_{B_{2R}-B_R} \Gamma_{,\alpha}(x-\xi)\,[f(\xi)-f(x)]\,d\xi,\ x \in B_R \tag{3.18}$$

$$U_{2,\alpha\beta}(x) = \int_{B_{2R}-B_R} \Gamma_{,\alpha\beta}(x-\xi)\,[f(\xi)-f(x)]\,d\xi$$

using Lemma 3.5 and the fact that $\Gamma_{,\alpha}(x-\xi) = -\partial\Gamma(x-\xi)/\partial\xi^\alpha$. From the second equation in (3.18) we see that

$$|\nabla^2 U_2(x)| \leqq Z_1(\mu) h_\mu(f)\,(R-|x|)^{\mu-1} \tag{3.19}$$

As in the proof of Lemma 3.6, it follows from (3.19) that

$$h_\mu(\nabla U_2) \leqq Z_2(\mu) h_\mu(f). \tag{3.20}$$

We let

$$U_{1\rho}(x) = \int_{B_{2R}-B(x,\rho)} \Gamma(x-\xi) f(\xi)\,d\xi,\ x \in B_R,\ 0 < \rho < R. \tag{3.21}$$

Then for such x and ρ,

$$U_{1\rho,\alpha}(x) = U_{3\rho\alpha}(x) + U_{4\rho\alpha}(x)$$

$$U_{3\rho\alpha}(x) = -\int_{\partial B(x,\rho)} \Gamma(x-\xi)[f(\xi)-f(x)]\,d\xi'_\alpha + C_\alpha f(x),$$

$$C_\alpha = -\int_{\partial B_1} \Gamma(y)\,dy'_\alpha$$

$$U_{4\rho\alpha}(x) = \int_{B_{2R}-B(x,\rho)} \Gamma_{,\alpha}(x-\xi) f(\xi)\,d\xi = \int_{B_{2R}-B(x,\rho)} \Gamma_{,\alpha}(x-\xi)[f(\xi)-f(x)]\,d\xi.$$

Clearly, as $\rho \to 0$, $U_{3\rho\alpha}(x)$ and $U_{4\rho\alpha}(x)$ converge uniformly on $\bar{B}_R$ to

$$U_{3\alpha}(x) = C_\alpha f(x), \quad U_{4\alpha} = \int_{B_{2R}} \Gamma_\alpha(x - \xi)[f(\xi) - f(x)]\,d\xi. \tag{3.22}$$

In fact,

$$|U_{4\rho\alpha}(x) - U_{4\alpha}(x)| \leqq Z_3(\mu) h_\mu(f) \cdot \rho^\mu, \quad Z_3 = Z_3(\mu, \nu, N, s, t, m_1, M). \tag{3.23}$$

But now, if $x, x_1, x_2, \bar{B}_R$,

$$\begin{aligned} U_{4\rho\alpha,\beta}(x) = &- \int_{\partial B(x,\rho)} \Gamma_{,\alpha}(x - \xi)[f(\xi) - f(x)]\,d\xi'_\beta \\ &+ \int_{B_{2R} - B(x,\rho)} \Gamma_{,\alpha\beta}(x - \xi)[f(\xi) - f(x)]\,d\xi \\ |\nabla U_{4\rho\alpha}(x)| \leqq Z_4(\mu) h_\mu(f) \cdot \rho^{\mu-1}, &\ |U_{4\rho\alpha}(x_2) - U_{4\rho\alpha}(x_1)| \\ &\leqq Z_4(\mu) \cdot h_\mu(f) \cdot \rho^\mu, \ |x_1 - x_2| = \rho. \end{aligned} \tag{3.24}$$

Assuming $x_1, x_2 \in \bar{B}_R$ and setting $|x_1 - x_2| = \rho$, we see from (3.22) and (3.23) that

$$h_\mu(U_{4\alpha}) \leqq Z_5(\mu) \cdot h_\mu(f), \quad h_\mu(U_{3\alpha}) \leqq Z_6(\mu) \cdot h_\mu(f). \tag{3.25}$$

The lemma follows.

4. Proofs of Theorems B and C.

In this section we prove Theorems B and C as stated in the introduction. We observe first:

LEMMA 4.1. *There is an* $h_0(\nu, N, s_j, t_j, m_1, M) > 0$ *such that, if* $0 < h \leqq h_0$, *then* $J(y)$ *is analytic for all complex* $y = y_1 + iy_2 \neq 0$ *for which* $|y_2| \leqq h\,|y_1|$; J *satisfies* (2.7) *and, either*

$$J(ky) = k^{m-\nu} J(y), \quad k \text{ real}, \ k > 0, \tag{4.1}$$

or else J *has the form* (2.6) *where* J_1 *is a polynomial of degree* $m - \nu\,(\geqq 0)$ *and* J_2 *satisfies* (4.1).

This follows directly from the homogeneity properties of J and Lemma 3.2.

GENERAL ASSUMPTION. *We shall assume that* h *is a fixed positive number such that* $0 < h \leqq h_0$.

We wish to show that if the $f_j(x)$ are analytic for $x \in B_{hR}$ and $f_j \in C^{\mu - s_j}$ on $\bar{B}_{hR}$, then the $F_j(x)$ as defined in (2.8) are analytic in B_{hR} and $F_j \in C^{m - s_j + \mu}$ on $\bar{B}_R$.

Remark. If $m=0$, these statements about the F_j are obvious, (2.13) holds and Theorem B follows. In this case, if u is a solution of (1.9) with $f_j=0$, we see that each term on the left in (1.9) is of class $C^{\mu-s_j}$, and hence, the operators L^{pj} may be applied to yield

$$Lu^p=0 \text{ or } u^p=0$$

since L is a constant $\neq 0$ and those $L^{pj}\neq 0$ are of order $-s_j-t_p\geqq 0$, Thus Theorem C holds. *Accordingly we assume $m>0$ for the remainder of this section.*

Now, we shall extend the functions $F_j(x)$ to the domains B_{hR} by a device used by E. E. Levi [5] and E. Hopf [4]. Let $x=x_1+ix_2\in B_{hR}$. For such x, define d_x as the distance of x from ∂B_{hR} (in 2ν-space) and ρ_x as the sup. of numbers $\rho>0$ such that all points x_1+s+ix_2 with $|s|<\rho$ belong to B_{hR}. Then, clearly

$$\rho_x=[(1+h^2)^{\frac{1}{2}}/h]d_x. \tag{4.2}$$

For such x, we define the ν-dimensional cone $S(x)$ by

$$\begin{aligned} S(x):\ \xi^\alpha=s^\alpha+i(1-\lambda)x_2^\alpha,\ \lambda=\lambda(s,x_1),\ 0\leqq\lambda\leqq 1,\\ (R^2-|x_1|^2)\lambda^2-2\lambda x_1\cdot(s-x_1)-|s-x_1|^2=0,\ s\in B_R\ (s\text{ real}). \end{aligned}\tag{4.3}$$

We note that $S(x)$ has a 1-1 projection on B_R, that λ is the ratio $|s-x_1|/|S-x_1|$ where S is the intersection of the ray $x_1 s$ with ∂B_R, that λ is real-analytic in (s,x_1) for $s\in B_R$, $x\in B_R$, $x\neq s$, and that the derivatives of λ are uniformly bounded if $s\neq x_1$, $x_1\in B_{R'}$, $R'<R$. Also, we note that

$$\begin{aligned} \lambda|x_2|&=(|s-x_1|/|S-x_1|)\,|x_2|\\ &\leqq(|s-x_1|/|S-x_1|)\cdot h\cdot(R-|x_1|)\leqq h\,|x_1-s|\\ (1-\lambda)|x_2|&\leqq(1-\lambda)h(R-|x_1|)\leqq h(R-|s|),\\ s&=(1-\lambda)x_1+\lambda S,\ S\in\partial B_R. \end{aligned}\tag{4.4}$$

The second of these follows since the maximum of $|(1-\lambda)x_1+\lambda S|$ for all S on ∂B_R and a given λ, $0<\lambda<1$, is taken on for S the nearest point to x_1. Thus, for any $s\neq x_1$ with $s\in B_R$, we see that ξ (as defined in (4.3)) $\in B_{hR}$ and that $[x_1-s+i\lambda x_2]$ belongs to the set where J is analytic. Thus, we may define

$$\begin{aligned} F_j(x)&=\int_{S(x)}J(x-\xi)f_j(\xi)\,d\xi\\ &=\int_{B_R}J[(x_1-s)+i\lambda x_2]\cdot f_j[s+i(1-\lambda)x_2]\,j(s,x)\,ds, \end{aligned}\tag{4.5}$$

where $j(s,x)=\partial(\xi^1,\cdots,\xi^\nu)/\partial(s^1,\cdots,s^\nu)=1-ix_2{}^\gamma\lambda_{s}{}^\gamma$, $x\in B_{hR}$.

Next, let us define

$$\lambda_\rho(s;x_1)=\lambda(s,x_1)[|s-x_1|-\rho]/[|s-x_1|-\rho\lambda(s,x_1)],\ x_1,s\in B_R,\ s\neq x_1;\quad 0<\rho<R-|x_1|.$$

We see that λ_ρ is real analytic for these values of (s,x_1), $\lambda_\rho=0$ for $|s-x_1|=\rho$, $\lambda_\rho=1$ for s on ∂B_R, and the derivatives of λ_ρ are uniformly bounded for $x_1\in B_{R'}$, $R'<R$, where they converge uniformly to those of λ as $\rho\to 0$. Finally we see, as above, that

$$\lambda_\rho|x_2|\leqq h|x_1-s|,\ (1-\lambda_\rho)|x_2|\leqq h(R-|s|),\quad s\in\bar B_R-B(x_1,\rho),\quad 0<\rho<\rho_x. \tag{4.6}$$

Accordingly, if we define $S_\rho(x)$ by

$$S_\rho(x):\ \xi^\alpha=s^\alpha+i(1-\lambda_\rho)x_2{}^\alpha,\ s\in\bar B_R-B(x_1,\rho),\quad 0<\rho<\rho_x, \tag{4.7}$$

then the points of $S_\rho(x)\in B_{hR}$ if x does. Thus, if f_j is analytic in B_{hR}, we may define

$$\begin{aligned}F_{\rho j}(x)&=\int_{S_\rho(x)}J(x-\xi)f_j(\xi)\,d\xi\\&=\int_{B_R-B(x_1,\rho)}J[(x_1-s)+i\lambda_\rho x_2]f_j[s+i(1-\lambda_\rho)x_2]j_\rho(s,x_1)\,ds,\\&\qquad x\in B_{hR},\ \rho_x>\rho.\end{aligned} \tag{4.8}$$

LEMMA 4.2. *Suppose* $x\in B_{hR}$, $0<\rho<\rho_x$, *and* ϕ *is analytic in a neighborhood of* $S_\rho(x)$. *Then*

$$\int_{S_\rho(x)}\phi_{,\alpha}(\xi)\,d\xi=\int_{\partial B_R}\phi(s)\,ds'_\alpha-\int_{\partial B(x_1,\rho)}\phi(s+ix_2)\,ds'_\alpha.$$

Proof. For the reader may verify that

$$\begin{aligned}\phi_{,\alpha}[s+i(1-\lambda_\rho)x_2]\cdot j_\rho(s,x_1)&=(\partial/\partial s^\alpha)\phi[s+i(1-\lambda_\rho)x_2]\\&\quad-ix_2{}^\beta\{(\partial/\partial s^\alpha)(\phi\lambda_{\rho,s^\beta})-(\partial/\partial s^\beta)(\phi\lambda_{\rho,s^\alpha})\},\end{aligned}$$

$$\lambda_{\rho,s^\beta}ds'_\alpha-\lambda_{\rho,s^\alpha}ds'_\beta=0,\ s\in\partial B_R,\ s\in\partial B(x_1,\rho).$$

LEMMA 4.3. *If the* f_j *are analytic in* B_{hR} *and* F_j *and* $F_{\rho j}$ *are defined as in* (4.5) *and* (4.8), *then* F_j *and* $F_{\rho j}$ *are analytic on their respective domains of definition and* $F_{\rho j}(x)$ *converges uniformly to* $F_j(x)$ *on any compact subset of* B_{hR} *as* $\rho\to 0$. *Moreover, the components of* $\nabla^{m-s_j-1}F_j$ *are given by* (3.5), *except that the last integral over the ball* B_R *is to be replaced by*

$$\int_{S(x)} \Gamma(x-\xi) f_{j,\beta_1\cdots\beta_n}(\xi)\,d\xi \qquad (n=-s_j), \tag{4.9}$$

the integral in (4.9) *being given by* (4.5) *with* J *replaced by* Γ. *Moreover,* Γ *satisfies the conditions of Lemma* 3.3 *for the complex* y *in Lemma* 4.1.

Proof. Since $m>0$, we see from Lemma 4.1 and the discussion of λ and λ_ρ that the $F_{\rho j}(x)$ converge uniformly to F_j on any compact subset of B_{hR}. Moreover, if $m>1$, the derivatives of $F_{\rho j}$ with respect to x_1^α and x_2^α converge similarly to those of F. We wish to show that F_j and $F_{\rho j}$ are analytic on B_{hR}. It is clear that we may approximate f_j and its derivatives of order $\leqq -s_j$ uniformly by functions $f_{jn}(x)=f_j[(1-n^{-1})x]$ which are analytic on $\bar{B}_{hR}$.

Differentiating (4.8), we see that (if $m>1$)

$$\begin{aligned} F_{\rho j,x_2^\alpha}(x_1+ix_2) &= \int_{B_R-B(x_1,\rho)} iJ_{,\alpha}\cdot f_j\cdot j_\rho\,ds \\ &\quad + \int_{B_R-B(x_1,\rho)} i\{(1-\lambda_\rho)\cdot j_\rho\cdot(Jf_{j,\alpha}-J_{,\alpha}f_j)-\lambda_{\rho s^\alpha}Jf_j\}\,ds \end{aligned} \tag{4.10}$$

$$\begin{aligned} F_{\rho j,x_1^\alpha}(x_1+ix_2) &= -\int_{\partial B(x_1,\rho)} Jf_jj_\rho\,ds'_\alpha + \int_{B_R-B(x_1,\rho)} \Gamma_{,\alpha}f_jj_\rho\,ds \\ &\quad + \int_{B_R-B(x_1,\rho)} -ix_2^\beta\{j_\rho\cdot\lambda_{\rho,x_1^\alpha}(Jf_{j,\beta}-J_{,\beta}f_j)+Jf_j\lambda_{\rho,s^\beta x_1^\alpha}\}\,ds, \end{aligned} \tag{4.11}$$

where the arguments in the functions are those in (4.8); here we have assumed that the f_j are analytic on $\bar{B}_{hR}$. The reader may verify that

$$\begin{aligned} -ix_2^\beta\{j_\rho\cdot\lambda_{\rho,x_1^\alpha}\cdot(Jf_{j,\beta}-J_{,\beta}f_j)+Jf_j\lambda_{\rho,s^\beta x_1^\alpha}\} &= (\partial/\partial s^\beta)(-ix_2^\beta Jf_j\lambda_{\rho,x_1^\alpha}) \\ i\{(1-\lambda_\rho)j_\rho(Jf_{j,\alpha}-J_{,\alpha}f_j)-\lambda_{\rho,s^\alpha}Jf_j\} &= (\partial/\partial s^\alpha)[i(1-\lambda_\rho)Jf_j] \\ &\quad + (\partial/\partial s^\alpha)[x_2^\beta(1-\lambda_\rho)\lambda_{\rho,s^\beta}Jf_j]-(\partial/\partial s^\beta)[x_2^\beta(1-\lambda_\rho)\lambda_{\rho,s^\alpha}Jf_j]. \end{aligned} \tag{4.12}$$

Using the facts that $\lambda_\rho(s,x_1)=0$ on $\partial B(x_1,\rho)$, $\lambda_\rho(s,x_1)=1$ for s on ∂B_R, so that $\lambda_{\rho,x_1^\alpha}=0$ for s on ∂B_R, and the relations (4.10)-(4.12), we obtain

$$\begin{aligned} F_{\rho j,x_2^\alpha}(x_1+ix_2) &= \int_{B_R-B(x_1,\rho)} iJ_{,\alpha}f_jj_\rho\,ds - i\int_{\partial B(x_1,\rho)} Jf_j\,ds'_\alpha \\ F_{\rho j,x_1^\alpha}(x_1+ix_2) &= \int_{B_R-B(x_1,\rho)} J_{,\alpha}f_jj_\rho\,ds - \int_{\partial B(x_1,\rho)} Jf_j\,ds'_\alpha. \end{aligned} \tag{4.13}$$

In obtaining these relations, we used the facts, implied by the fact that $\lambda_\rho(s,x_1)=0$ for all $x_1\in B_{R-\rho}$ and all s on $\partial B(x_1,\rho)$, that

$$(4.14)\qquad \lambda_{\rho,x_1^\alpha}(s,x_1) = -\lambda_{\rho,s^\alpha}(s,x_1),\quad \lambda_{\rho,s^\alpha}\,ds'_\beta - \lambda_{\rho,s^\beta}\,ds'_\alpha = 0,\qquad s \in \partial B(x_1,\rho).$$

The result (4.13) shows that the $F_{\rho j}$ are analytic and that

$$(4.15)\quad F_{\rho j,\alpha}(x) = \int_{S_\rho(x)} J_{,\alpha}(x-\xi) f_j(\xi)\,d\xi - \int_{\partial B(x_1,\rho)} J(x_1 - s) f_j(s + ix_2)\,ds'_\alpha,$$

all provided that the f_j are analytic on $\bar{B}_{hR}$.

In case the f_j are analytic on $\bar{B}_{hR}$, we wish to show that

$$(4.16)\qquad F_{\rho j,\alpha}(x) = -\int_{\partial B_R} J(x-s) f_j(s)\,ds'_\alpha + \int_{S_\rho(x)} J(x-\xi) f_{j,\alpha}(\xi)\,d\xi.$$

But (4.16) follows from (4.15) and Lemma 4.2. The restriction that f_j be be analytic on $\bar{B}_{hR}$ is easily replaced by the restrictions as stated. As in Lemma 3.3, the process may be repeated. Finally we may let $\rho \to 0$.

As in Section 3, our desired results concerning the F_j will follow from our study of the functions U and W_γ defined by

$$(4.17)\qquad U(x) = \int_{S(x)} \Gamma(x-\xi) f(\xi)\,d\xi,\ f \in C^{0+\mu} \text{ on } \bar{B}_{hR},$$

$$x \in B_{hR}$$

$$(4.18)\qquad W_\gamma(x) = -\int_{\partial B_R} \Gamma(x-s) f(s)\,ds'_\gamma,\ f \in C^{q+\mu} \text{ on } \bar{B}_{hR},$$

where f is analytic on B_{hR} in both vases and Γ satisfies

Condition A. $\Gamma(y)$ is analytic for all complex $y = y_1 + iy_2 \neq 0$ in which $|y_2| \leqq h|y_1|$ and Γ satisfies (3.7) and

$$(4.19)\qquad \Gamma(ky) = k^{1-\nu}\Gamma(y),\ k \text{ real},\ k > 0,$$

for such y.

LEMMA 4.4. *The first two results of Lemma* 3.5 *hold for* $x \in B_h(x_0, R)$, *the set of all* $x = x_1 + ix_2$ *such that* $|x_2 - x_{02}| \leqq h(R - |x_1 - x_{01}|)$, $x_0 = x_{01} + ix_{02}$. *The third result is replaced by*

$$\int_{S_\rho(x)} \Gamma_{,\alpha_1\cdots\alpha_n}(x-\xi)\cdot(\xi^{\beta_1} - x^{\beta_1})\cdots(\xi^{\beta_p} - x^{\beta_p})\,d\xi = 0,\ p < n,\ x \in B_{hR}.$$

LEMMA 4.5. *Suppose* Γ *satisfies Condition* A, $f \in C^{q+\mu}$ *for real* x *on* $\bar{B}_{hR}$ *and* W_γ *is defined by* (4.18). *Then* $W_\gamma(x)$ *is analytic on* B_{hR} *and* $W_\gamma \in C^{q+\mu}$ *on* $\bar{B}_{hR}$ *and*

$$h^*_\mu(\nabla^q W_\gamma) \leqq K_{6q}(h,\mu)\cdot h_\mu(\nabla^q f).$$

Proof. It is obvious that W_γ is analytic on B_{hR}. Differentiating $q+1$ times and using Lemma 4.4, we obtain

$$\nabla^{q+1}W_\gamma(x) = -\int_{\partial B_R} \nabla^{q+1}\Gamma(x-\xi)\,[f(\xi) - \sum_{j=0}^{q} \nabla^j f(x_1)\cdot(\xi - x_1)^j/j!]\,d\xi'_\gamma,$$
$$x = x_1 + ix_2 \in B_{hR}.$$

From Condition A, we see that

$$|\nabla^{q+1}\Gamma(y)| \leqq Z_1(h)\cdot \|y\|^{-\nu-q} \text{ for } |y_2| \leqq h\,|y_1|,\ y \neq 0.$$

Since $|x_2| \leqq h(R - |x_1|)$, we see that

$$|\xi - x_1| \leqq \|\xi - x\| = [\,|\xi - x_1|^2 + |x_2|^2]^{\frac{1}{2}} \leqq (1+h^2)^{\frac{1}{2}}\,|\xi - x_1|.$$

The remainder of the proof of Lemma 3.6 may now be carried over.

LEMMA 4.6. *If f is analytic on B_{hR} and $f \in C^\mu$ on $\bar{B}_{hR}$, then*

$$|\nabla f(x)| \leqq K_7 h^*_\mu(f)\cdot d_x^{\mu-1},\ |\nabla^2 f(x)| \leqq K_8 h^*_\mu(f)\cdot d_x^{\mu-2},\ x \in B_{hR},$$

where K_7 and K_8 depend only on ν and h.

Proof. Clearly there is a constant κ, $0 < \kappa < 1$, which depends only on ν and h that the polycylinder $|\xi^\alpha - x^\alpha| < \kappa d_x$, $\alpha = 1,\cdots,\nu$, lies in B_{hR}. Since $f \in C^\mu$, we have

$$f(x) = (2\pi i)^{-\nu}\int_\gamma \cdots \int_\gamma f(\xi)\,d\xi^1\cdots d\xi^\nu/(\xi^1 - x^1)\cdots(\xi^\nu - x^\nu),$$
$$(\gamma : |\xi - x| = \kappa d_x)$$

$$\bar{\zeta}^\alpha f_{,\alpha}(x) = (2\pi i)^{-\nu}\int_\gamma \cdots$$
$$\int_\gamma \bar{\zeta}^\alpha[f(\xi) - f(x)]\,d\xi^1\cdots d\xi^\nu/[(\xi^1 - x^1)\cdots(\xi^\nu - x^\nu)(\xi^\alpha - x^\alpha)]$$

for any complex ζ^α. The result follows from the fact that

$$|(\xi^\alpha - x^\alpha)^{-1}\bar{\zeta}^\alpha| \leqq \|\zeta\|\cdot(\kappa d_x)^{-1}.$$

The second result is proved similarly.

LEMMA 4.7. *If f satisfies the conditions of Lemma 4.6 and U is defined by (4.17), then U is analytic on B_{hR} and $U \in C^{1+\mu}$ on $\bar{B}_{hR}$ with*

$$U_{,\alpha}(x) = C_\alpha f(x) + \int_{S(x)} \Gamma_{,\alpha}(x-\xi)\,[f(\xi) - f(x)]\,d\xi, \tag{4.20}$$

$$h^*_\mu(\nabla U) \leqq K_9(h,\mu)\,h^*_\mu(f). \tag{4.21}$$

Proof. Define $U_\rho(x) = \int_{S_\rho(x)} \Gamma(x-\xi) f(\xi)\, d\xi$. Then, we may proceed as in the proof of Lemma 4.3 to obtain

$$\begin{aligned} U_{\rho,\alpha}(x) &= \int_{S_\rho(x)} \Gamma_{,\alpha}(x-\xi) f(\xi)\, d\xi - \int_{\partial B(x_1,\rho)} \Gamma(x_1 - s) f(s + ix_2)\, ds'_\alpha \\ &= \int_{S_\rho(x)} \Gamma_{,\alpha}(x-\xi)\, [f(\xi) - f(x)]\, d\xi + C_\alpha f(x) \qquad (4.22) \\ &\quad - \int_{\partial B(x_1,\rho)} \Gamma(x_1 - s)\, [f(s + ix_2) - f(x_1 + ix_2)]\, ds'_\alpha . \end{aligned}$$

(4.20) follows from the second line of (4.22) by letting $\rho \to 0$.

Let $V_\alpha(x)$ denote the integral in (4.20) and let

$$V_{\rho\alpha}(x) = \int_{S_\rho(x)} \Gamma_{,\alpha}(x-\xi)\, [f(\xi) - f(x)]\, d\xi = \int_{S_\rho(x)} \Gamma_{,\alpha}(x-\xi) f(\xi)\, d\xi ;$$

we have seen that $V_{\rho\alpha}(x) \to V_\alpha(x)$ for $x \in B_{hR}$. Now let $\sigma = \rho_x/2$, $0 < \rho < \sigma$. Then, differentiating as above and using Cauchy's integral theorem, we obtain

$$\begin{aligned} V_{\rho\alpha,\beta}(x) &= \int_{B(x_1,\sigma)-B(x_1,\rho)} \Gamma_{,\alpha\beta}(x_1 - s)\, [f(s + ix_2) - f(x_1 + ix_2) \\ &\qquad\qquad - (s^\gamma - x_1{}^\gamma) f_{,\gamma}(x)]\, ds \\ &\quad + \int_{B_R - B(x_1,\sigma)} \Gamma_{,\alpha\beta}[(x_1 - s) + i\lambda_\sigma x_2]\, \{f[s + i(1-\lambda_\sigma)x_2] - f(x)\}\, j_\sigma(s, x_1)\, ds \qquad (4.23) \\ &\quad - \int_{\partial B(x_1,\rho)} \Gamma_{,\alpha}(x_1 - s)\, [f(s + ix_2) - f(x_1 + ix_2) - (s^\gamma - x^\gamma) f_{,\gamma}(x)]\, ds'_\beta \\ &\qquad\qquad + C^\gamma{}_{\alpha\beta} f_{,\gamma}(x). \end{aligned}$$

Since f is analytic in B_{hR}, we may let $\rho \to 0$ to obtain

$$\begin{aligned} V_{\alpha,\beta}(x) &= C^\gamma{}_{\alpha\beta} f_{,\gamma}(x) + \int_{B(x_1,\sigma)} \Gamma_{,\alpha\beta}(x_1 - s) \\ &\qquad \times [f(s + ix_2) - f(x_1 + ix_2) - (s^\gamma - x_1{}^\gamma) f_{,\gamma}(x)]\, ds \qquad (4.24) \\ &\qquad + \int_{S_\sigma(x)} \Gamma_{,\alpha\beta}(x-\xi)\, [f(\xi) - f(x)]\, d\xi , \end{aligned}$$

where the last integral in (4.24) is the middle one in (4.23).

Now, for $s \in B(x_1, \sigma)$, $d_\xi \geqq d_x/2$ where $\xi = s + ix_2$. Hence

$$\| f(s + ix_2) - f(x) - (s^\gamma - x_1{}^\gamma) f_{,\gamma}(x) \| \leqq \tfrac{1}{2} K_8 2^{2-\mu} d_x{}^{\mu-2}\, | s - x_1 |^2 ,$$

using Lemma 4.6. Hence, since $| x_1 - s | \leqq \| x - \xi \| \leqq (1 + h^2)^{\frac{1}{2}}\, | x_1 - s |$, we see that

$$(4.25)\qquad |\nabla V_\alpha(x)| \leqq Z_1(h,\mu)\, h^*_\mu(f)\, d_x^{\mu-1}.$$

The desired Hölder continuity of V_α on $\bar{B}_{hR}$ follows from the fact that any two points y and z in B_{hR} can be joined by an arc $x = x(s)$, $0 \leqq s \leqq l$, such that

$$\int_0^l d_{x(s)}{}^{\mu-1}\, ds \leqq Z_2(h)\cdot \| y - z \|^{\mu}\cdot \mu^{-1}$$

The result (4.21) follows.

We now prove Theorem C.

THEOREM C. *Suppose u^k is of class $C^{t_k+\mu}$ for x real and on $\bar{B}_{hR}$ and satisfies* (1.9) *there with $f_j = 0$. Then u^k can be extended to be analytic on B_{hR} and of class $C^{t_k+\mu}$ on $\bar{B}_{hR}$ with*

$$h^*_\mu(\nabla^{t_k}u^k) \leqq K_3(h,\mu)\, h_\mu(\nabla^{t_k}u^k).$$

Proof. Let us define $U^k(x) = \int_{B_R} J(x-\xi)u^k(\xi)\,d\xi$, $x \in \bar{B}_R$. Then U^k is of class $C^{m+t_k+\mu}$ on $\bar{B}_R$ and satisfies $LU^k(x) = u^k(x)$ there. Let us define $F_j(x) = L_{jk}U^k(x)$, $x \in B_R$. Then if $m > 1$, we obtain

$$\begin{aligned} U^k{}_{,\alpha}(x) &= \int_{B_R} J_{,\alpha}(x-\xi)u^k(\xi)\,d\xi = -\int_{B_R} u^k(\xi)\,(\partial/\partial\xi^\alpha)J(x-\xi)\,d\xi \\ &= -\int_{\partial B_R} J(x-\xi)u^k(\xi)\,d\xi'_\alpha + \int_{B_R} J(x-\xi)u^k{}_{,\alpha}(\xi)\,d\xi; \end{aligned}$$

one obtains the same result if $m = 1$ by approximating by U_ρ, etc., as in the proof of Lemma 3.7. By repeating this process, we see (since $L_{jk}u^k = 0$) that $F_j(x)$ is a sum of terms of the form

$$C\cdot \int_{\partial B_R} J_{,\alpha_1\cdots\alpha_n}(x-\xi)u^k{}_{,\beta_1\cdots\beta_p}(\xi)\,d\xi'_\gamma,\quad n+p+1 = s_j + t_k$$

(there are no terms with $s_j + t_k = 0$). Now if the L^{qj} are defined as near (2.14), then $u^q(x) = L^{qj}F_j(x)$ and u^q is a sum of terms of the form

$$C\cdot \int_{\partial B_R} J_{,\alpha_1\cdots\alpha_n}(x-\xi)u^k{}_{,\beta_1\cdots\beta_p}(\xi)\,d\xi'_\gamma,\ n+p = m + t_k - t_q - 1,\ p \leqq t_k - 1.$$

If $n \geqq m-1$, the result follows from Lemma 4.5; if $n < m-1$, one can differentiate $m-1-n$ times and then apply Lemma 4.5.

UNIVERSITY OF CALIFORNIA.

REFERENCES.

[1] S. Bernstein, " Sur la nature analytique des solutions des équations aux dérivées partièlles due second ordre," *Mathematische Annalen*, vol. 59 (1904), pp. 20-76.

[2] ———, " Demonstration du théorème de M. Hilbert sur la nature analytique des solutions des equations du type elliptique sans l'emploi des séries normales," *Mathematische Zeitschrift*, vol. 29 (1928), pp. 330-348.

[3] A. Douglas and L. Nirenberg, " Interior estimates for elliptic systems of partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 503-538.

[4] A. Friedman, " Classes of solutions of linear non-hyperbolic differential equations," (to appear in the *Journal of Mathematics and Mechanics*).

[5] M. Gevrey, " Démonstration du théorème de Picard-Bernstein par la méthode des contours successifs; prolongement analytique," *Bulletin des Sciences Mathématiques*, (2) vol. 50 (1926), pp. 113-128.

[6] E. Hopf, " Über den funktionalen, insbesondere den analytischen Charakter der Lösungen elliptischer differentialgleichungen zweiter ordnung," *Mathematische Zeitschrift*, vol. 34 (1932), pp. 194-233.

[7] E. E. Levi, " Sulle equazioni lineari totalemente ellittiche alle derivate parziali," *Palermo Rendiconti*, vol. 24 (1907), pp. 275-317.

[8] H. Lewy, " Neuer Beweis des analytischen Charakters der Lösungen elliptischer Differentialgleichungen," *Mathematische Annalen*, vol. 101 (1929), pp. 609-619.

[9] S. Mandelbrojt, *Séries de Fourier et classes quasi-analytiques de fonctions*, Collection Borel, Paris, 1935.

[10] C. B. Morrey, Jr. and L. Nirenberg, " On the analyticity of the solutions of linear elliptic systems of partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 10 (1957), pp. 271-290.

[11] L. Nirenberg, " Remarks on strongly elliptic partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 648-674.

[12] I. Petrowsky, " Sur l'analyticité des solutions des systèmes d'équations différentielles," *Rec. Math. N. S. Mat. Sbornik* 5(47), (1939), pp. 3-70.

[13] T. Radó, " Das Hilbertsche Theorem über den analytischen Charakter der Lösungen der partiellen Differentialgleichungen zweiter Ordnung," *Mathematische Zeitschrift*, vol. 25 (1926), pp. 514-589.

ON THE ANALYTICITY OF THE SOLUTIONS OF ANALYTIC NON-LINEAR ELLIPTIC SYSTEMS OF PARTIAL DIFFERENTIAL EQUATIONS.*[1]

By Charles B. Morrey, Jr.

PART II. Analyticity at the Boundary.

5. Introduction; strongly elliptic systems; outline of the proof. In this part, we shall show that a solution of a *strongly elliptic* (in the sense of Nirenberg, [5]) analytic system, which possesses Dirichlet data which are analytic along an analytic portion of the boundary of its domain of definition, can be extended analytically across that portion of the boundary.

The analyticity of the solutions of general analytic elliptic systems on the interior of their domains of definition has been proved in Part I [4] where a more extensive introduction and bibliography are given. We number the sections of Part II serially after those of Part I. Avner Friedman [1] has recently extended the results of Parts I and II to obtain corresponding results for quasi-analytic systems and the still more general systems in which the ϕ_j belong to the M_n classes of Mandelbrojt [3].

Since such a system remains analytic and strongly elliptic under an analytic transformation of the independent variables, we may choose any point on our portion of the boundary and transform the part of the domain and its boundary analytically onto that part of the hemisphere

$$G_R : |x|^2 + y^2 < R^2, y > 0, \ x = (x^1, \cdots, x^\nu), \ \nu \geqq 1, \ R = R_0 > 0, \tag{5.1}$$

in such a way that the given point corresponds to the origin. Throughout this chapter, we shall let Σ_R be the part of the boundary ∂G_R of G_R for which $y > 0$ and σ_R denote that part for which $y = 0$. At times we shall let $X = (x, y)$, $X^\alpha = x^\alpha$, $\alpha \leqq \nu$, $X^{\nu+1} = y$.

The system (1.1) is said to be strongly elliptic at the vector function $u_0(X)$ if and only if the corresponding equations of variation form a strongly elliptic linear system as defined by Nirenberg in [5]:

---

* Received September 30, 1957.

[1] The research reported in this paper was partially supported by Contract Nonr-222(37) with the Office of Naval Research.

$$L_{jk}(X, D)u^k = f_j, \qquad j, k = 1, \cdots, N. \tag{5.2}$$

Here L_{jk} is an operator of order $\leqq s_j + t_k$, where we now assume, with Nirenberg, that $s_j = t_j \geqq 0$, $j = 1, \cdots, N$ and assume that there is an $m_2 > 0$ such that

$$\operatorname{Re}[L^0_{jk}(X, \Lambda)\xi^j\bar{\xi}^k] \geqq m_2 \sum_{j=1}^{N} |\Lambda|^{2s_j} |\xi_j|^2, \quad m_2 > 0 \tag{5.3}$$

for all real $\Lambda = (\lambda^1, \cdots, \lambda^{\nu-1})$ and all complex ξ; the coefficients in L may be complex; $L^0_{jk}(X, D)$ is the part of L_{jk} which is of order exactly $s_j + s_k$. The condition (5.3) guarantees that each operator L_{jj} is strongly elliptic of order $2s_j$. In case some $s_j = 0$, one may clearly solve the j-th equation of the non-linear system for u^j in terms of the others and the remaining system is easily seen to be strongly elliptic. Thus we shall assume that each $s_j > 0$ and shall define

$$s = \max s_j, \quad s_0 = \min s_j \qquad (0 < s_0 \leqq s). \tag{5.4}$$

Now, suppose P_0 is a given point of our boundary and u is a given solution of (1.1) in which u^k is of class $C^{s+s_k+\mu}$ $(0 < \mu < 1)$ near P_0 up to the boundary and such that

$$\nabla^p u^k(P) = g^{pk}(P), \qquad 0 \leqq p \leqq s_k - 1, \tag{5.5}$$

where the $g^{pk}(P)$ are analytic along the boundary near P_0. As in the first paragraph, we may assume $P_0 = 0$, σ_{R_0} to be the given portion of the boundary and $G_{R_0} \cup \sigma_{R_0}$ to be the given neighborhood of P_0. By subtracting off an analytic function of x only, we may assume that

$$D_y^p u^k(x, 0) = 0, \quad 0 \leqq p \leqq s_k - 1, \qquad k = 1, \cdots, N. \tag{5.6}$$

Definition. A vector u satisfying (5.6) will be said to possess 0 *Dirichlet data along* σ_{R_0}.

Next, we write

$$u^k(x, y) = Q^k(x, y) + v^k(x, y) \qquad (k = 1, \cdots, N), \tag{5.7}$$

where Q^k is that polynomial of degree $s + s_k$ which possesses 0 Dirichlet data along σ_{R_0} and such that

$$\nabla^p Q^k(0, 0) = \nabla^p u^k(0, 0), \qquad 0 \leqq p \leqq s + s_k. \tag{5.8}$$

Then, as in Section 1, we make the substitution (5.7) in the system (1.1) and rewrite the system in the form

$$L_{jk}v^k = M_{jk}v^k + \chi_j(x, y, \cdots, v^k, \nabla v^k, \cdots, \nabla^{s_j+s_k}v^k, \cdots), \tag{5.9}$$

where now L_{jk} is the operator of order exactly $s_j + s_k$ with coefficients evaluated at $(0,0)$, M_{jk} contains the lower order terms with constant coefficients, and χ_j is what remains. Since

$$(5.10) \qquad \nabla^p v^k(0,0) = 0, \qquad 0 \leqq p \leqq s + s_k,$$

we may differentiate the j-th equation in (5.9) $s - s_j$ times with respect to the X^α and conclude that the Taylor expansion of χ_j begins with a homogeneous polynomial in X of degree $s - s_j + 1$, linear terms in the $\nabla^p v^k$ with coefficients homogeneous and linear in X, and quadratic terms in the $\nabla^p v^k$ with constant coefficients.

In addition to the notations of Part I, we shall use the following: As in (5.1), we often consider functions (or tensors) $u(x,y)$, $x = (x^1, \cdots, x^\nu)$, y being a single variable. Then $D^p u$ and $D_x{}^p u$ will denote any p-th partial derivative or any such involving only differentiation with respect to the x^α; such a derivative may also be denoted by $u_{,\alpha_1 \cdots \alpha_p}$; $\nabla^p{}_x u$ shall denote the tensor $u_{,\alpha_1 \cdots \alpha_p}$. For $0 < h < 1$, we let G_{hR} denote the set of all (x,y) such that y is real with $0 < y < R$ and $x = x_1 + ix_2$ is complex and $x \in B_{hR'}$ with $R' = \sqrt{(R^2 - y^2)}$.

The remainder of the proof is very similar to that in Section 1. In Section 7, we introduce a Green's function for the half-space E^+ where $y \geqq 0$, for the system

$$(5.11) \qquad L_{jk} u^k = f_j$$

which enables us to prove the analogs, Theorems A′, B′, and C′, of the Theorems A, B, and C of Part I. We define the space E_R and $\| u \|$ as in Section 1 with $\bar{B}_R$ replaced by $\bar{G}_R$ and t_k replaced by $s + s_k$ and E_{R0} as the subset of those u in E_R which possess 0 Dirichlet data on σ_R. We also define the space F_R of vectors $f_j \in C^{s - s_j + \mu}$ with $\nabla^p f_j(0,0) = 0$ for $0 \leqq p \leqq s - s_j$ and $\| f \| = \sup_j h_\alpha(\nabla^{s - s_j} f_j)$. We next define the spaces $E^*{}_{hR}$ and $E^*{}_{hR0}$ as the subsets of E_R and E_{R0}, respectively, in which each $u^k(x,y)$ is analytic in x for $(x,y) \in G_{hR}$ and $u^k \in C^{s + s_k + \mu}$ in (x,y) on $\bar{G}_{hR}$ with $\| u \|^*{}_h = \sup_k h^*{}_\mu(\nabla^{s + s_k} u^k)$; the space $F^*{}_{hR}$ is defined analogously.

The analogs of Theorems A, B, and C become:

THEOREM A′. *For each $R > 0$, there exists a bounded linear operator $P_{R0}(f)$ with bound $\leqq K_9(\mu)$ from F_R to E_{R0} such that, if $u = P_{R0}(f)$, then u is a solution of (5.11) on G_R.*

THEOREM B′. *There is a number $h_1 = h_1(\nu, N, s_j, m_2, M) > 0$ such that, if $f \in F_{hR}$ with $0 < h \leqq h_1$ and $u = P_{R0}(f)$, then u can be extended to $\in H^*{}_{hR0}$ on $\bar{G}_{hR}$ and $\| P_{R0}(f) \|^*{}_h \leqq K_{10}(\mu, h) \| f \|^*{}_h$.*

THEOREM C'. *If* $H_R \in E_{R0}$ *on* $\bar{G}_R$ *and* H_R *is a solution of the homogeneous equations* (5.11) *on* G_R, *then* H_R *can be extended to* $\in E^*_{hR0}$ *on any* $\bar{G}_{hR}$ *with* $0 < h \leqq h_1$ *with* $\| H_R \|^*_h \leqq K_{11}(h,\mu) \| H_R \|$.

The operator $T_R(V_R; H_R)$ can then be defined as in Section 1 and is seen to have the corresponding properties to (1.16) in the spaces E_{R0} and E^*_{hR0}. Thus, as in Section 1, we conclude that any solution v in E_{R0} on $\bar{G}_R$ of (5.9) $\in E^*_{hR0}$ on $\bar{G}_{hR}$ for any $h \leqq h_1$. But this implies that

$$(5.12) \qquad | \nabla^n{}_x D_y{}^p u^k | \leqq A(LR^{-1})^n n!, \qquad n = 0, 1, 2, \cdots, 0 \leqq p \leqq s + s_k,$$

for all real (x, y) with $|x| \leqq R/2$ and $0 \leqq y \leqq R/2$. Since u is analytic for $y > 0$ by Part I, the proof of the Cauchy-Kowalewski theorem shows that corresponding bounds to (5.12) hold for *all* the derivatives including those with respect to y.

6. Certain systems of ordinary differential equations. In this section, we study certain solutions of systems of ordinary differential equations of the form

$$(6.1) \qquad \sum_{k=1}^{N} \sum_{p=0}^{s_j+s_k} b_{jkp} \cdot (-i)^p D^p u^k(y) = f_j(y), \qquad j = 1, \cdots, N,$$

on the interval $[0, \infty)$. The coefficients are required to satisfy

$$(6.2) \qquad \begin{gathered} \operatorname{Re} \sum_{j,k=1}^{N} \Big[\sum_{p=0}^{s_j+s_k} b_{jkp} \mu^p \Big] \xi^j \bar{\xi}^k \geqq m_2 \sum_{j=1}^{N} (1+\mu^2)^{s_j} |\xi^j|^2, \qquad m_2 > 0, \\ \sum_{j,k=1}^{N} \sum_{p=0}^{s_j+s_k} | b_{jkp} |^2 \leqq M^2, \end{gathered}$$

for any real μ and any complex ξ; the coefficients may be complex.

We define H_0 as the set of all vectors u in which u^k is of class C^{s_k-1} with $D^{s_k-1}u^k$ absolutely continuous and

$$(6.3) \qquad D^p u^k(0) = 0, \qquad 0 \leqq p \leqq s_k - 1,$$

and for which the norm $\| u \|$ $(\geqq 0)$ defined by

$$(6.4) \qquad \| u \|^2 = \int_0^\infty \sum_{j=1}^{N} \sum_{p=0}^{s_j} C_p{}^{s_j} | D^p u^j |^2 \, dy < \infty.$$

Clearly H_0 is a Hilbert space. For u and v having finite norm (not necessarily in H_0), we define

$$(6.5) \qquad \begin{aligned} B(u,v) = \int_0^\infty \sum_{j.k=1}^{N} \{ \bar{v}^j \sum_{p=0}^{s_k} b_{jkp} (-i)^p D^p u^k \\ + \sum_{p=s_k+1}^{s_k+s_j} b_{jkp} (-i)^p (-1)^{p-s_k} D^{s_k} u^k D^{p-s_k} \bar{v}^j \} \, dy. \end{aligned}$$

We also define $B_a{}^b(u, v)$ in the same way with $[0, \infty)$ replaced by $[a, b]$.

LEMMA 6.1. *Any solution of the homogeneous equations* (6.1) *is the sum of exponential functions with possible polynomial coefficients. If u is a vector in which u^k is of class C^{s_k-1} on the interval $[a, b]$ with $D^{s_k-1}u^k$ absolutely continuous with $D^{s_k}u^k$ in $\mathcal{L}_2$ there and if $B_a{}^b(u, v) = 0$ for every v of the same type with $D^p v^k(a) = D^p v^k(b) = 0$ for $0 \leqq p \leqq s_k - 1$, then u is a solution of the homogeneous equations* (6.1).

Proof. The first statement is easily proved by restricting u to an arbitrary interval $[a, b]$ and then taking Fourier transforms. To prove the second, we note that a function v of the type required is uniquely determined by a vector w in $\mathcal{L}_2$ on $[a, b]$ in which

$$\begin{aligned} &\int_a^b ((b-y)^p/p!)w^j(y)\,dy = 0 \quad \text{for } p = 0, \cdots, s_j - 1, \\ (6.6) \qquad &v^j(y) = \int_a^y ((y-\eta)^{s_j-1}/(s_j-1)!)w^j(\eta)\,d\eta. \end{aligned}$$

By inserting v^j as defined by (6.6) in $B_a{}^b(u, v)$ and interchanging order of integration and the letters y *and* η, we obtain

$$\int_a^b \sum_{j=1}^N A_j(y)\bar{w}_j(y)\,dy = 0$$

for all w satisfying (6.6), $A_j(y)$ being defined in (6.7). It follows that there are constants d_{jp} such that

$$\begin{aligned} A_j(y) \equiv \sum_{k=1}^N \{ & b_{jk,s_j+s_k} i^{s_j}(-i)^{s_k} D^{s_k}u^k(y) \\ & + \sum_{p=0}^{s_k} b_{jkp}(-i)^p \int_y^b ((\eta-y)^{s_j-1}/(s_j-1)!)D^p u^k(\eta)\,d \\ (6.7) \qquad & + \sum_{p=s_k+1}^{s_j+s_k-1} b_{jkp}(-i)^p(-1)^{p-s_k} \\ & \times \int_y^b ((\eta-y)^{s_j+s_k-1-p}/(s_j+s_k-1-p)!)D^{s_k}u^k(\eta)\,d\eta\} \\ & = \sum_{p=0}^{s_j-1} d_{jp}(b-y)^p/p!. \end{aligned}$$

From (6.2), it follows that the determinant of the coefficients b_{jk,s_j+s_k} is not zero, so the $D^{s_k}u^k(y)$ can be expressed in terms of the other terms. Since these are all continuous we see first that the $D^{s_k}u^k$ are continuous and then that all the derivatives are continuous. Differentiating the j-th equation in (6.7) s_j times, $j = 1, \cdots, N$, we see that u satisfies the homogeneous equations (6.1).

THEOREM 6.1. *Suppose that the* $f_j(y)$ *are of class* C^{s-s_j} *on* $[0,\infty)$ *and suppose* $f_j(y)=0$ *for* $y \geqq Y$ (>0). *Then there is a unique solution* u^k *of class* C^{s+s_k} *of* (6.1) *in which* $u \in H_0$. *Also* u^k *varies analytically with the coefficients* b_{jkp} *over the convex set defined by* (6.2).

Proof. Now, suppose u and $v \in H_0$. Introducing the Fourier transforms

$$U^k(z)=(2\pi)^{-\frac{1}{2}}\int_0^\infty e^{-iyz}u^k(y)\,dy, \qquad V^j(z)=(2\pi)^{-\frac{1}{2}}\int_0^\infty e^{-iyz}v^j(y)\,dy,$$

we see that

$$B(u,v)=\int_{-\infty}^{\infty}\sum_{j,k=1}^{N}\Big[\sum_{p=0}^{s_j+s_k} b_{jkp}z^p\Big]U^k\bar{V}^j\,dz. \tag{6.8}$$

From (6.8) and (6.2) we see that

$$\operatorname{Re}B(u,v)\geqq m_2\int^{\infty}\sum_{j=1}^{N}(1+z^2)^{s_j}\,|\,U^j\,|^2\,dz=m_2\,\|\,u\,\|^2. \tag{6.9}$$

Now, let Tu and w be defined in terms of u and f by

$$(Tu,v)=B(u,v),\ (w,v)=\int_0^\infty f_j\bar{v}^j\,dy,\ \ v\in H_0. \tag{6.10}$$

From (6.2), it follows that T is a bounded linear operator. From a lemma of Lax and Milgram ([2], p. 169), it follows that T has an inverse and that $\|\,T^{-1}\,\|\leqq m_2^{-1}$. Now the equations $Tu=v$ and

$$B(u,v)=\int_0^\infty f_j\bar{v}^j\,dy \text{ for all } v\in H_0 \tag{6.11}$$

are equivalent. Accordingly there is a unique solution u in H_0 of (6.11). Since T is analytic (linear, in fact) in the coefficients b_{jkp}, it follows that u is for each fixed f.

Finally, if we write the equations (6.1) in the form $l_{jk}u^k=f_j$, let $l(\mu)$ be the determinant of the $l_{jk}(\mu)$, let F_j be a solution of $l(D)F_j=f_j$, and set $u_1{}^k=l^{kl}F_l$, where $l^{jk}(\mu)$ is the cofactor of $l_{kj}(\mu)$; then u_1 is a solution of (6.1) with the stated differentiability properties. Obviously, this solution satisfies (6.11) with the interval $[0,\infty)$ replaced by $[0,Y]$ for any Y. Clearly the difference $u-u_1$ satisfies $B_0{}^Y(u-u_1,v)=0$ for all v as in Lemma 6.1 so that $u-u_1$ is a solution of the homogeneous equations (6.1) Thus u has the differentiability properties as stated.

THEOREM 6.2. *There exist unique vector solutions* $u_m{}^q$ $(=u_m{}^{kq})$ *of the homogeneous equations* (6.1), *each having finite norm as defined in* (6.4) *and satisfying the initial conditions*

$$(6.12)\qquad D^p u_m{}^{kq}(0) = \delta_m{}^k \delta_q{}^p,\quad k, m = 1, \cdots, N,\quad 0 \leqq p \leqq s_k - 1,$$
$$0 \leqq q \leqq s_m - 1.$$

These solutions depend analytically on the coefficients b_{jkp} on the convex set of b_{jkp} satisfying (6.2).

Proof. For, let $u_{0m}{}^q$ be any vector class C^∞ vanishing for $y \geqq 1$ and satisfying the given initial conditions; we assume that $u_{0m}{}^q$ is independent of the b_{jkp}. From Theorem 6.1, it follows that there exists a unique solution $u_{1m}{}^q$ in H_0 of equations (6.1) with $f_{mj}{}^q = L_{jk} u_{0m}{}^{kq}$. The vector $u_m{}^q = u_{0m}{}^q - u_{1m}{}^q$ satisfies the given conditions. If $u_{2m}{}^q$ were another such, then $u_{2m}{}^q - u_m{}^q$ would satisfy the homogeneous equations (6.1) and would belong to H_0 and would therefore vanish by Theorem 6.1.

LEMMA 6.2. *There are rectangles R^+, $R_1{}^+$, R^-, and $R_1{}^-$ with $R^+ \cup \partial R^+$ in the upper half-plane, with $R^- \cup \partial R^-$ symmetrically located in the lower half-plane, with $R_1{}^\pm \cup \partial R_1{}^\pm$ interior to $R^\pm$ and symmetrically placed, which depend only on ν, N, s_j, m_2, and M, such that for any set of coefficients satisfying* (6.2), *all the roots of* $L(z) = 0$ (see below) *with positive imaginary parts lie in $R_1{}^+$ and all those with negative imaginary parts lie in $R_1{}^-$, there being $s_1 + \cdots + s_N$ roots of each type.*

Proof. This is obvious since the set of all complex coefficients satisfying (6.2) is compact and convex, the roots of $L(z) = 0$ vary continuously with the coefficients, no root is real, and the set contains the particular array of coefficients

$$b_{jj,2q} = C_q{}^{s_j}, \qquad b_{jkp} = 0 \text{ otherwise}.$$

Now, let us define the functions

$$(6.13)\qquad \hat{u}_m{}^{kq}(z) = (2\pi)^{-1} \int_0^\infty u_m{}^{kq}(u) e^{-iuz}\, du,\quad \mathcal{J}(z) < \epsilon,$$

$\hat{u}_m{}^{kq}(z)$ being defined wherever possible by analytic extension, and let

$$(6.14)\qquad L_{jk}(z) = \sum_{p=0}^{s_j+s_k} b_{jkp} z^p,$$

L^{kl} be the cofactor of L_{lk} and

$$(6.15)\qquad L(z) = \det \| L_{jk}(z) \|, \qquad M^{kl}(z) = L^{-1}(z) L^{kl}(z).$$

Then we have the following results:

THEOREM 6.3. *The $\hat{u}_m{}^{kq}$ are rational functions of z which are analytic* *for* z *outside* R_1^+ *and whose coefficients vary analytically with the coefficients* b_{jkp} *over the set* (6.2). *We have*

$$u_m^{kq}(u) = \int_{\partial R^+} e^{iuz}\hat{u}_m^{kq}(z)\,dz, \quad u \geqq 0, \tag{6.16}$$

$$L_{jk}(z)\hat{u}_m^{kq}(z) = P_{jm}^{q}(z), \tag{6.17}$$

$$\int_{\partial R^+}(iz)^p\hat{u}_m^{kq}(z)\,dz = \delta^{pq}\delta_m^k \text{ if } 1 \leqq k, m \leqq N,\ 0 \leqq p < s_k,\quad 0 \leqq q < s_m, \tag{6.18}$$

$$(iz)^pM^{kl}(z) - \sum_{m=1}^{N}\sum_{q=0}^{s_m-1}\hat{u}_m^{kq}(z)\int_{\partial R^+}(i\zeta)^{p+q}M^{ml}(\zeta)\,d\zeta = P^{pkl}(z), \tag{6.19}$$

where the P_{jm}^q *are polynomials (or* $\equiv 0$*) and the* P^{pkl} *are rational functions which are analytic outside of* R_1^-.

Proof. The first statement follows from the form of the u_m^{kq} and their analytic dependence on the coefficients and (6.13). (6.16) also follows by writing out what u_m^{kq} is explicitly. To prove (6.17), we use the facts that the u_m^{kq} are solutions of the homogeneous equations (6.1) and the $\hat{u}_m^{kq}$ are rational functions. (6.18) follows from (6.16) and (6.12). To prove (6.19), let P^{pkl} denote the left side of (6.19) and define

$$v^{kl}(u) = \int_{\partial R^+} e^{iuz}M^{kl}(z)\,dz, \quad U^{pkl}(u) = \int_{\partial R^+} e^{iuz}P^{pkl}(z)\,dz. \tag{6.20}$$

We see that the vector v^l and all of its derivatives are solutions of finite norm of the homogeneous equations (6.1) and then that

$$U^{pkl}(u) = D^pv^{kl}(u) - \sum_{m=1}^{N}\sum_{q=0}^{s_m-1} u_m^{kq}(u)D^{p+q}v^{ml}(0), \tag{6.21}$$

so that the vectors U^{pl} are also solutions of finite norm of the homogeneous equations (6.1). Also

$$D^rU^{pkl}(0) = D^{p+r}v^{kl}(0) - \sum_{m=1}^{N}\sum_{q=0}^{s_m-1} D^ru_m^{kq}(0)D^{p+q}v^{ml}(0) = 0, \quad 0 \leqq r < s_k,$$

by virtue of (6.12). Hence the $U^{pkl}(u) \equiv 0$ from which the result follows.

7. The Green's matrix; proof of Theorems A′, B′, and C′. In this section, we define the Green's matrix alluded to in Section 5 and prove Theorems A′, B′, and C′. We may write the operator

$$L_{jk} = \sum_{p=0}^{s_j+s_k}\sum_{\alpha} a_{jkp}^{\alpha_1\cdots\alpha_p}D_y^{s_j+s_k-p}D_x^{\alpha_1}\cdots D_x^{\alpha_p} \tag{7.1}$$

and we define the operator

$$L^*_{jk} = (-1)^{s_j+s_k} L_{jk}. \tag{7.2}$$

If u^k and v^j are sufficiently smooth on a sufficiently smooth domain D, we see that

$$\int_D \sum_{j,k=1}^{N} [v^j L_{jk} u^k - u^k L^*_{jk} v^j]\, dx dy = \int \sum_{\alpha=1}^{\nu+1} B^\alpha(u,v) n_\alpha\, dS, \tag{7.3}$$

where each $B^\alpha(u,v)$ is a sum of terms of the form

$$c D^p u^k D^q v^j, \text{ where } p + q = s_j + s_k - 1; \tag{7.4}$$

the B^α are not unique but we select particular ones.

We define the functions $u_m^{kq}(z,\sigma)$, $L_{jk}(z,\sigma)$, $L^{kl}(z,\sigma)$, $M^{kl}(z,\sigma)$ and $L(z,\sigma)$ by (6.3) through (6.15) with the b_{jkp} replaced by

$$b_{jkp}(\sigma) = \sum_\alpha a_{jkn}{}^{\alpha_1 \cdots \alpha_n} \sigma_{\alpha_1} \cdots \sigma_{\alpha_n}, \; n = s_j + s_k - p, \; \sigma = (\sigma_1, \cdots, \sigma_\nu). \tag{7.5}$$

For any σ with $|\sigma| = 1$, we see that

$$\begin{aligned} \operatorname{Re} \sum_{j,k=1}^{N} \left[\sum_{p=0}^{s_j+s_k} b_{jkp}(\sigma) \mu^p \right] \xi^j \bar{\xi}^k &= \operatorname{Re} \sum_{j,k=1}^{N} L_{jk}(\sigma,\mu) \xi^j \bar{\xi}^k \\ &\geqq m_2 \sum_{j=1}^{N} (1+\mu^2)^{s_j} |\xi_j|^2, \; m_2 > 0 \end{aligned} \tag{7.6}$$

by virtue of the strong ellipticity condition (5.3). Thus (6.2) holds for all such σ and we see that all the $\hat{u}_m{}^{kq}(z,\sigma)$ are also analytic in σ near σ real with $|\sigma| = 1$.

Next, we define the functions $J_h(w)$ by

$$J_h(w) = \begin{cases} h!(-iw)^{-h-1}, & h \geqq 0 \\ ((iw)^{-h-1}/(-h-1)!)[-\log(-iw) + C_{-h-1}], & h < 0 \end{cases} \tag{7.7}$$
$$C_0 = 0, \; C_t = 1 + 1/2 + \cdots + 1/t \text{ if } t \geqq 1,$$

where for the log, we cut the w plane along the negative imaginary axis and take the principal log. We note that

$$D^p J_h(w) = i^p J_{h+p}(w). \tag{7.8}$$

Now, let us define

$$\begin{aligned} \Gamma^{kl}(x,y) &= C_1{}^{kl} \int_\Sigma \{ \pm \int_{\partial R^\pm} M^{kl}(z,\sigma) J_{\nu-s_k-s_l}(\sigma \cdot x + yz)\, dz \}\, d\Sigma_\sigma \\ C_1{}^{kl} &= (2\pi)^{-\nu-1} i^{-s_k-s_l}, \; \Sigma : |\sigma| = 1, \; y \neq 0, \end{aligned} \tag{7.9}$$

the sign being that of y (defining $\Gamma^{kl}(x,0)$ by continuity),

$$(7.10)\quad \begin{aligned} H^{kl}(x,y,\eta) &= C_1^{kl}\int_\Sigma d\Sigma \int_{\partial R^+} dz \int_{\partial R^-} N^{kl}(z,\zeta,\sigma) \\ &\qquad \times J_{\nu-s_k-s_l}(\sigma\cdot x+yz-\eta\zeta)\,d\zeta, \\ N^{kl}(z,\zeta,\sigma) &= \sum_{m=1}^{N}\sum_{q=0}^{s_m-1} \hat{u}_m^{kq}(z,\sigma)(i\zeta)^q M^{ml}(\zeta,\sigma), \end{aligned}$$

$$(7.11)\qquad G^{kl}(x,y,\eta) = \Gamma^{kl}(x,y-\eta) + H^{kl}(x,y,\eta),$$

$$(7.12)\quad \begin{aligned} J^*(x,y) = (-1)^{S+P}(2\pi)^{-\nu-1}\int_\Sigma \{\pm \int_{\partial R^\pm} &(1+z^2)^{-P}L^{-1}(z,\sigma) \\ &\times J_{\nu-2S-2P}(\sigma\cdot x+yz)\,dz\}\,d\Sigma, \end{aligned}$$

$$(7.13)\qquad M(x,y) = LJ^*(x,y),$$

$$(7.14)\qquad \Gamma^{*kl}(x,y) = L^{kl}J^*(x,y),$$

where, in (7.12), P is taken so large that $\nu+s_k-s_l-2P<-1$ for all k,l.

Remark. The case $\nu=1$ is special in the sense that Σ consists of the two points $\sigma=\pm 1$ and we interpret $\int_\Sigma f(\sigma,\cdots)\,d\Sigma$ in this case as simply $f(1,\cdots)+f(-1,\cdots)$ in (7.9), (7.10), and (7.12). In what follows, we shall treat only the case $\nu>1$ leaving the case $\nu=1$ to the reader.

Definition. A function $f(x)$ is said to be *essentially homogeneous of degree* p if and only if $p<0$ implies that f is positively homogeneous of degree p and $p\geqq 0$ implies that

$$(7.15)\qquad f(X) = f_0(X)\log|X| + f_1(X),$$

where f_1 is positively homogeneous of degree p and f_0 is a homogeneous polynomial of degree p (or $\equiv 0$).

THEOREM 7.1. *There is an* $h_2(\nu,N,s_j,m_2,M)>0$ *such that* $J^*(X)$ *is analytic for all complex* $X=X_1+iX_2\neq 0$ *for which* $|X_2|\leqq h_2|X_1|$. *For such* X, J^* *is essentially homogeneous of degree* $2S+2P-\nu-1$. *Furthermore*

$$(7.16)\qquad \Delta^{P-1}M(X) = \Gamma_0(X),\quad \Delta^P M(X) = 0,$$

$$(7.17)\qquad \Delta^P\Gamma^{*kl}(X) = \Gamma^{kl}(X), \qquad\qquad X\neq 0$$

$$(7.18)\qquad L_{jk}\Gamma^{*kl}(X) = L_{kj}\Gamma^{*lk}(X) = \delta_j^{\,l}M(X),$$

Proof. The essential homogeneity of J^* is obvious. If $y\neq 0$, we may replace $\pm\int_{\partial R^\pm}$ by $\int_{-\infty}^{\infty}$ in (7.12). By introducing new variables τ on the unit sphere S in $(\nu+1)$ space by

$$\tau^{\alpha}=\sigma^{\alpha}(1+z^2)^{-\frac{1}{2}}, \qquad \tau^{\nu+1}=z(1+z^2)^{-\frac{1}{2}}$$

and noting that $dz d\Sigma=(1+z^2)^{(\nu+1)/2}\,dS$, we see that we may write J^* in the form

$$\begin{aligned}J^*(X)&=(2\pi i)^{-\nu-1}\int_S L^{-1}(\tau)\cdot((\tau\cdot X)^{2S+2P-\nu-1}/(2S+2P-\nu-1)\,!)\\&\quad\times[C_{2S+2P-\nu-1}+\log(1-(\tau^{\nu+1})^2)^{\frac{1}{2}}-\log(-i\tau\cdot X)]\,dS_\tau.\end{aligned}\tag{7.19}$$

The first two terms in the bracket in (7.19) yield homogeneous polynomials in X of the desired degree. The analyticity of J^* follows as in Section 3.

Using (7.12) and (7.14), we see that

$$\begin{aligned}\Gamma^{*kl}(x,y)&=(-1)^P C_1^{kl}\int_\Sigma\{\pm\int_{\partial R^\pm}(1+z^2)^{-P}M^{kl}(z,\sigma)\\&\quad\times J_{\nu-s_k-s_l-2P}(\sigma\cdot x+yz)\,dz\}\,d\Sigma,\end{aligned}\tag{7.20}$$

from which (7.17) follows easily. Next,

$$\begin{aligned}\sum_k L_{jk}\Gamma^{*kl}(x,y)&=Z_1\int_\Sigma\{\pm\int_{\partial R^\pm}(1+z^2)^{-P}\delta_j{}^l J_{\nu+s_j-s_l-2P}(\sigma\cdot x+yz)dz\}\,d\Sigma\\&=\delta_j{}^l M(x,y),\ \ Z_1=(-1)^P i^{s_j-s_l}(2\pi)^{-\nu-1}.\end{aligned}$$

Likewise

$$\sum_k L_{kj}\Gamma^{*lk}(x,y)=\delta_j{}^l M(x,y)$$

$$\begin{aligned}M(x,y)&=(-1)^P(2\pi)^{-\nu-1}\int_\Sigma\{\pm\int_{\partial R^\pm}(1+z^2)^{-P}J_{\nu-2P}(\sigma\cdot x+yz)dz\}\,d\Sigma\\&=(2\pi i)^{-\nu-1}\int_S((\tau\cdot X)^{2P-\nu-1}/(2P-\nu-1)\,!)\\&\quad\times[C_{2P-\nu-1}+\log\surd[1-(\tau^{\nu+1})^2]-\log(-i\tau\cdot X)]\,dS_\tau\end{aligned}\tag{7.21}$$

To prove (7.16), we first consider the case $\nu=2k$. Then

$$\begin{aligned}\Delta^{P-k-1}M(X)&=(2\pi i)^{-\nu-1}\int_S(\tau\cdot X)\\&\quad\times[1+\log\surd[1-(\tau^{\nu+1})^2]-\log(-i\tau\cdot X)]\,dS_\tau.\end{aligned}$$

In order to evaluate this, we set $\tau\cdot X=|X|\cos\phi$ and the integral becomes

$$\begin{aligned}&-(2\pi i)^{-\nu-1}\Gamma_\nu|X|\int_0^\pi\sin^{2k-1}\phi\cos\phi\log(-i\cos\phi)\,d\phi,\\&\Gamma_\nu=\nu\pi^{\nu/2}/\Gamma(1+\nu/2).\end{aligned}\tag{7.22}$$

In (7.22), we may replace the segment from 0 to π by any path with the same endpoints for which $\mathfrak{I} \cos\phi \geqq 0$ and > 0 when $R \cos\phi = 0$. Then, integrating by parts, etc., (7.22) becomes

$$-(2\pi i)^{-2k-1}(2k)\pi^k/k!\cdot(-\pi i/2k)\,|X| = (-1)^k(\pi^{-k}\cdot 2^{-2k-1}/k!)\,|X|.$$

Thus

$$\Delta^{P-1}M(X) = -2^k\cdot k!\cdot 1\cdot 3\cdots(2k-3)r^{1-2k}/\pi^k 2^{2k+1}k! = \Gamma_0(X)$$

$$(\Gamma_0(X) = -(\Gamma(k+3/2)/(2k-1)(2k+1)\pi^{k+1/2})\,|X|^{1-2k}, \text{ see } (2.9))$$

in this case, The case where $\nu = 2k+1$ is treated similarly.

Lemma 7.1. *The function*

$$F_{vrh}(z,\zeta,\sigma,A) = \int_{B_A} \xi^{\beta_1}\cdots\xi^{\beta_r}\,d\xi \times \int_0^\infty \eta^h J_{\nu+2+v}(-\sigma\cdot\xi + z - \eta\zeta)\,d\eta, \quad r+h \leqq v+1, \tag{7.23}$$

is uniformly bounded for all z on ∂R^+, ζ on ∂R^-, $|\sigma| = 1$, and real $A \geqq 0$ and tends to zero as $A \to +\infty$ for each set of (z,ζ,σ) as described.

Proof. Since $\mathfrak{I}(z - \sigma\cdot\xi) > 0$ and $\mathfrak{I}(\zeta) < 0$, we see that

$$\int_0^\infty \eta^h J_{\nu+2+v}(-\sigma\cdot\xi + z - \eta\zeta)\,d\eta = Z_1(-\zeta)^{-h-1}(z-\sigma\cdot\xi)^{h-\nu-2-v}.$$

To evaluate

$$\int_{B_A} \xi^{\beta_1}\cdots\xi^{\beta_r}(z-\sigma\cdot\xi)^{h-\nu-2-v}\,d\xi \tag{7.24}$$

for a given σ with $|\sigma| = 1$, first make a rotation of axes from ξ to $'\xi$ so that $\sigma\cdot\xi = {'\xi^1}$ and then set $|\xi| = |'\xi| = \rho$, $'\xi^1 = \rho\cos\phi$ and the integral in (7.24) becomes a sum of terms of the form

$$c(\sigma)\int_0^\pi \sin^{\nu-2+s}\phi\cos^{r-s}\phi\,d\phi \int_0^A \rho^{r+\nu-1} \times (-\rho\cos\phi + z)^{h-\nu-2-v}\,d\rho. \tag{7.25}$$

In each of the terms in (7.25), we may replace the segment from 0 to π by a path γ such that $-\cos\phi$ describes the upper half circle from -1 to 1. Then (7.25) becomes

$$c_1(\sigma)z^{r+h-2-\nu}\int_\gamma \tan^{\nu-2+s}\phi\sec^2\phi \times \left[\int_0^{-A\cos\phi/z} \tau^{r+\nu-1}(\tau+1)^{h-\nu-2-v}\,d\tau\right]d\phi. \tag{7.26}$$

Since $r+h \leqq v+1$, the result follows from the form (7.26).

THEOREM 7.2. *There is an* $h_1(\nu, N, s_j, m_2, M)$ *with* $0 < h_1 \leqq h_2$ *such that* $\Gamma^{kl}(x, y)$ *is analytic for all complex* $X = X_1 + iX_2 \neq 0$ *with* $|X_2| \leqq h_1 |X_1|$ *and* $H^{kl}(x, y, \eta)$ *is analytic for all complex*

$$(x_1 + ix_2, y_1 + iy_2, \eta_1 + i\eta_2) \neq (0, 0, 0)$$

such that $y_1 \geqq 0$, $\eta_1 \geqq 0$, *and*

$$(|x_2|^2 + y_2^2 + \eta_2^2) \leqq h_1^2(|x_1|^2 + y_1^2 + \eta_1^2).$$

Γ^{kl} *and* H^{kl} *are essentially homogeneous of degree* $s_k + s_l - \nu - 1$ *in their arguments on the domain above. We also have the formulas*

$$L_{jk}(X)\Gamma^{kl}(X) = L_{jk}(X)H^{kl}(X, \Xi) = 0; \tag{7.27}$$

$$L^*_{jk}(\Xi)\Gamma^{lj}(X - \Xi) = L^*_{jk}(\Xi)H^{lj}(X, \Xi) = 0; \tag{7.28}$$

$$D_y^p G^{kl}(x, 0, \eta) = D_\eta^r G^{kl}(x, y, 0) = 0, \ \eta > 0, y > 0, \ 0 \leqq p < s_k, \ 0 \leqq r < s_l. \tag{7.29}$$

$$\int_{E^+} D^2 D_y^v \omega(-\xi, y, \eta)\eta^h \xi^{\beta_1 \cdots \beta_r} d\xi d\eta = 0 \ \textit{for} \ h + r \leqq v + 1, \ h, r \geqq 0, \text{ where } \omega = D^{s_k + s_l - 1}(H_y^{kl} + H_\eta^{kl}). \tag{7.30}$$

Finally, if $f_j \in C^{s - s_j + \mu}$ *on* $\bar{G}_a$ *and* u *is a solution of* (5.11) *in which* $u^k \in C^{s + s_k + \mu}$ *on* $\bar{G}_a$, *then*

$$u^l(X) = \int_{G_a} G^{lj}(X, \Xi) f_j(\Xi) d\Xi - \int_{\partial G_a} B^\alpha[G^l(X, \Xi), u(\Xi)] n_\alpha dS. \tag{7.31}$$

Proof. The analyticity of Γ^{kl} follows from Theorem 7.1. The analyticity of H^{kl} for real $(x, y, \eta) \neq (0, 0, 0)$ with $y \geqq 0$, $\eta \geqq 0$, $y + \eta > 0$ is obvious from (7.10). To remove the restriction y or $\eta > 0$ with $x \neq 0$, let $x_0 \neq 0$ and make a rotation $\sigma = \sigma(\tau, \xi)$, $\xi = x/|x|$, from σ to τ which is analytic in x for x near x_0 so that $\sigma \cdot x = |x| \tau^1$, then let

$$\tau^1 = \cos\phi, \ \tau^{1+\alpha} = \omega^\alpha \sin\phi, \ |\omega| = 1,$$

$$N_1^{kl}(z, \zeta, \phi, \xi) = \sin^{\nu-2}\phi \int_{|\omega|=1} N^{kl}[z, \zeta, \sigma(\cos\phi, \omega\sin\phi, \xi)] dS_\omega;$$

the expression for H^{kl} then becomes

$$C_1^{kl} \int_0^\pi d\phi \int_{\partial R^+} dz \int_{\partial R^-} N_1^{kl}(z, \zeta, \phi, \xi) J_{\nu - s_k - s_l}(|x|\cos\phi + yz - \eta\zeta) d\zeta. \tag{7.32}$$

The segment $[0, \pi]$ in (7.32) may be replaced by a nearby path γ on which $\mathcal{I}\cos\phi > 0$ except at the endpoints, N_1 being analytic in its arguments. The essential homogeneity is obvious.

The first of the formulas in (7.27) and (7.28) follow from Theorem 7.1. Since $i^{s_j+s_k}C_1^{kl} = i^{s_j-s_l}(2\pi)^{-\nu-1}$ and

$$L_{jk}(z,\sigma)N^{kl}(z,\zeta,\sigma) = \sum_{m,q}(i\zeta)^q M^{ml}(\zeta,\sigma)P^q{}_{jm}(z,\sigma)$$

we see that the second formula of (7.27) holds. Now

$$\begin{aligned} L^*{}_{jk}(\xi,\eta)H^{lj}(x-\xi,y,\eta) &= i^{s_k-s_l}(2\pi)^{-\nu-1}\int_\Sigma d\Sigma \int_{\partial R^+} dz \\ &\times \int_{\partial R^-} L_{jk}(\zeta,\sigma)N^{lj}(z,\zeta,\sigma)J_{\nu+s_k-s_l}(\sigma\cdot x + yz - \eta\zeta)\,d\zeta = 0, \end{aligned}$$

since $L_{jk}(\zeta,\sigma)N^{lj}(z,\zeta,\sigma) = \sum_{q=0}^{s_k-1}\hat{u}_k{}^{lq}(z,\sigma)(i\zeta)^q$.

Now, the first of (7.29) follows easily since

$$\begin{aligned} &\int_{\partial R^+}(iz)^p N^{kl}(z,\zeta,\sigma)\,dz \\ &\qquad = \sum_{m,q}(i\zeta)^q M^{ml}(\zeta,\sigma)\int_{\partial R^+}(iz)^p \hat{u}_m{}^{kq}(z,\sigma)\,dz = (i\zeta)^p M^{kl}(\zeta,\sigma) \end{aligned}$$

using (7.10) and (6.18). The second result in (7.29) follows from (7.10) and (6.19) with $p = r$ since

$$\int_{\partial R^-}(i\zeta)^r N^{kl}(z,\zeta,\sigma)\,d\zeta = -\int_{\partial R^+}(i\zeta)^r N^{kl}(z,\zeta,\sigma)\,d\zeta$$

on account of the restrictions on q and r and the degrees of the rational functions involved.

To prove (7.30), we note that

$$\begin{aligned} &D^2 D_y{}^v \omega(-\xi,y,\eta) \\ &\qquad = \int_\Sigma d\Sigma \int_{\partial R^+} dz \int_{\partial R^-}\phi(z,\zeta,\sigma)J_{\nu+2+v}(-\sigma\cdot\xi + yz - \eta\zeta)\,d\zeta, \end{aligned}$$

where ϕ is a polynomial in (z,ζ,σ) times N^{kl}. On account of the homogeneity, we may assume $y = 1$; and the integral in (7.30) is absolutely convergent so that it may be written in the form

$$\lim_{A\to\infty}\int_\Sigma d\Sigma \int_{\partial R^+} dz \int_{\partial R^-}\phi(z,\zeta,\sigma)F_{vrh}(z,\sigma,A)\,d\zeta = 0$$

by Lemma 7.1.

To prove (7.31), we first notice that all the derivatives occurring in $L_{jk}(X)\Gamma^{*lj}(X-\Xi)$ are continuous at $\Xi = X$ on account of our choice of P in (7.12) and we may apply (7.3) with $D = G_a$ and $v^j = \Gamma^{*lj}$ to obtain

$$(7.33)\qquad \int_{G_a} M(X-\Xi)u^l(\Xi)\,d\Xi = \int_{G_a} \Gamma^{*lj}(X-\Xi)f_j(\Xi)\,d\Xi - \int_{\partial G_a} B^\alpha[\Gamma^{*l}(X-\Xi), u(\Xi)]n_\alpha\,dS_\Xi$$

since

$$L^*_{jk}(\Xi)\Gamma^{*lj}(X-\Xi) = L_{jk}(X)\Gamma^{*lj}(X-\Xi) = \delta_k{}^l M(X-\Xi).$$

By operating on both sides of (7.33) with $\Delta^P(X)$, we obtain

$$(7.34)\qquad u^l(X) = \int_{G_a} \Gamma^{lj}(X-\Xi)f_j(\Xi)\,d\Xi - \int_{\partial G_a} B^\alpha[\Gamma^l(X-\Xi), u(\Xi)]n_\alpha\,dS_\Xi.$$

Applying (7.3) with $D = G_a$ and $v^j = H^{lj}$, we obtain

$$(7.35)\qquad 0 = \int_{G_a} H^{lj}(X-\Xi)f_j(\Xi)\,d\Xi - \int_{\partial G_a} B^\alpha[H^l(X,\Xi), u(\Xi)]n_\alpha\,dS_\Xi.$$

The result follows by adding (7.34) and (7.35).

THEOREM 7.3. *Suppose $f_j(x,y) \in C^{s-s_j+\mu}$ on E^+ and vanishes outside G_a and suppose that*

$$(7.36)\qquad u^k(x,y) = \int_{E^+} G^{kl}(x-\xi, y, \eta)f_l(\xi,\eta)\,d\xi d\eta \text{ for } y > 0.$$

Then $u^k \in C^{s+s_k+\mu}$ on E^+, u is a solution of (5.11) for $y > 0$, u has 0 Dirichlet data on $y = 0$ and

$$\sup_k h_\mu(\nabla^{s+s_k}u^k) \leqq K_{12}(\mu) \sup_l h_\mu(\nabla^{s-s_l}f_l).$$

If, also, $f_j(x,y)$ is analytic in x for $(x,y) \in G_{hR}$ and $\in C^{s-s_j+\mu}$ on $\bar{G}_{hR}$ for some R with $0 < R \leqq a$ and h with $0 < h \leqq h_1$, then u^k can be extended to be analytic in x on G_{hR} and of class $C^{s-s_k+\mu}$ on G_{hR} and

$$\sup_k h^*_\mu(\nabla^{s+s_k}u^k) \leqq K_{13}(h,\mu) \sup_l h^*_\mu(\nabla^{s-s_l}f_l) \text{on } \bar{G}_{hR}.$$

Proof. From the essential homogeneity of Γ^{kl} and H^{kl}, it follows that we can differentiate (7.36) p times $(0 \leqq p \leqq s_k - 1)$ with respect to y and set $y = 0$ under the integral sign; that u^k has 0 Dirichlet data then follows from (7.29).

Next choose (x_0, y_0) and ρ with $0 < \rho < y_0$ and let $u^k(x,y) = v^k(x,y) + w^k(x,y)$, where

$$w^k(x,y) = \int_{B(x_0,y_0,\rho)} \Gamma^{kl}(x-\xi, y-\eta)f_l(\xi,\eta)\,d\xi d\eta.$$

It is easy to see that v is analytic inside $B(x_0, y_0, \rho)$ and is a solution of the homogeneous equations (5.11) there and that

$$(7.37) \qquad w^k(X) = \sum_l \Delta^P L^{kl} F_l(X), F_l(X) = \int_{B(X_0,\rho)} J^*(X - \Xi) f_l(\Xi)\, d\Xi.$$

Using the methods of Part I, one easily establishes that $F_l \in C^{2P+2S+s-s_l+\mu}$ $(S = s_1 + \cdots + s_N)$ so that $w^k \in C^{s+s_k+\mu}$. From (7.37), the essential homogeneity, and Theorem 7.1, we see that

$$\begin{aligned} L_{jk} w^k(X) &= \sum_l \Delta^P [L_{jk} L^{kl} F_l(X)] = \Delta^P L F_j(X) \\ &= \Delta^P \int_{B(X_0,\rho)} M(X - \Xi) f_j(\Xi)\, d\Xi = f_j(X). \end{aligned}$$

Thus $u^k \in C^{s-s_k+\mu}$ and u is asolution of (5.11) for $y > 0$.

To show that $u^k \in C^{s+s_k+\mu}$ for $y \geqq 0$, we differentiate each term (l fixed) of (7.36) $s + s_k - 1$ times. We note that as long as ϕ is differentiable, we may write

$$(7.38) \qquad \begin{aligned} D_{x^\alpha} \int_{E^+} G^{kl}(x-\xi, y, \eta) \phi(\xi,\eta)\, d\xi d\eta &= -\int_{E^+} D_{\xi^\alpha} G^{kl} \phi\, d\xi d\eta \\ &= \int_{E^+} G^{kl}(x-\xi, y, \eta) D_{\xi^\alpha} \phi(\xi,\eta)\, d\xi d\eta \\ D_y \int_{E^+} G^{kl} \phi\, d\xi d\eta &= \int_{E^+} [\Omega^{kl}\phi + G^{kl} D_\eta \phi(\xi,\eta)]\, d\xi d\eta, \\ \Omega^{kl} = D_y G^{kl} + D_\eta G^{kl} &= D_y H^{kl} + D_\eta H^{kl}. \end{aligned}$$

So by first applying the devices of (7.38) $s - s_l$ times to the l-th term of (7.36), we see that any $D^{s+s_k-1} u^k$ is a sum of terms of the form

$$(7.39) \qquad \begin{gathered} \int_{E^+} g(x-\xi, y, \eta)\, \phi(\xi,\eta)\, d\xi d\eta \text{ or } \int_{E^+} D_y{}^v \omega(x-\xi, y, \eta)\, \psi(\xi,\eta)\, d\xi d\eta, \\ \phi \in C^\mu, \ \psi \in C^{v+1+\mu}, \ g = D^{s_k+s_l-1} G^{kl}, \end{gathered}$$

and ω is given by (7.30) and $\phi = 0$ outside G_a.

First, we note that any second derivative of a term of the second type in (7.39) is of the form

$$\begin{aligned} &\int_{E^+} D^2 D_y{}^v \omega\, (x-\xi, y, \eta) [\psi(\xi,\eta) - \sum_{w=0}^{\nu-1} \nabla^w \psi(x, 0) \cdot (\Xi - X)^w / w!]\, d\xi d\eta \\ &\qquad + \sum_{r+h \leqq v+1} [D_y{}^h \psi_{,\beta_1 \cdots \beta_r}(x, 0) \\ &\qquad\qquad \times \int_{E^+} \xi^{\beta_1} \cdots \xi^{\beta_r} \eta^h D^2 D_y{}^v \omega(-\xi, y, \eta)\, d\xi d\eta] / (r+h)! \end{aligned}$$

and all the last terms vanish on account of (7.30). The first term in (7.39) can be written in the form

$$\begin{aligned}\int_{B_a}\gamma(x-\xi,y-\eta)\phi^*(\xi,\eta)d\xi d\eta-\int_{E^-}\gamma(x-\xi,y-\eta)\phi^*(\xi,\eta)d\xi d\eta\\ +\int_{E^+}h(x-\xi,y,\eta)\phi(\xi,\eta)d\xi d\eta=I_1+I_2+I_3\end{aligned}\tag{7.40}$$

where $\phi^*(\xi,\eta)=\phi(\xi,\eta)$ if $\eta\geqq 0$ and $\phi^*(\xi,\eta)=\phi(\xi,-\eta)$ if $\eta\leqq 0$ and γ and h are corresponding derivatives of G^{kl} and H^{kl}, respectively. The first term I_1 in (7.40) is of class $C^{1+\mu}$ on $\bar{B}_a$ with desired Hölder bounds on its first derivatives by Lemma 3.7. Next, any second derivative of I_2 in (7.40) involving at least one differentiation with respect to an x^α can be written in the form

$$\int_{E^-}DD_x\gamma(x-\xi,y-\eta)[\phi^*(\xi,\eta)-\phi^*(x,y)]d\xi d\eta$$

so that

$$|DD_xI_2|\leqq Z_1(\mu,\nu,N,s_j,m_2,M)\cdot h_\mu(\phi)\cdot y^{\mu-1}.\tag{7.41}$$

In like manner, we see that

$$|DD_xI_3|\leqq Z_2(\mu,\nu,N,s_j,m_2,M)\cdot h_\mu(\phi)\cdot y^{\mu-1}.\tag{7.42}$$

Thus we see that any derivative $D_xD^{s+s_k-1}u^k\in C^\mu$ for $y\geqq 0$ with

$$h_\mu(D_xD^{s+s_k-1}u^k)\leqq Z_3(\mu,\nu,N,s_j,m_2,M)\sup_j h_\mu(\nabla^{s-s_j}f_j).\tag{7.43}$$

But u is a solution of (5.11) for $y>0$. The ellipticity of (5.11) allows us to differentiate the j-th equation of (5.11) $s-s_j$ times with respect to y and then solve for $D_y{}^{s+s_k}u^k$ in terms of the other derivatives so that such derivatives also $\in C^\mu$ and bounds like those in (7.43) hold for those derivatives also.

Now, if each f_j can also be extended to be analytic in x for (x,y) in G_{Rh} with $f_j\in C^{s-s_j+\mu}$ in $\bar{G}_{Rh}$, $0<R\leqq a$, $0<h\leqq h_1$, then the u^k can also be extended to be analytic in x for (x,y) on G_{Rh} by merely replacing the part of the range of integration on (ξ,η) for which $(\xi,\eta)\in G_R$ by the manifold $S_{Rh}(x,y)$: η real with $0<\eta<R$ and ξ on the cone with vertex at x and outer boundary $\partial B_{R'}$ with $R'=(R^2-\eta^2)^{\frac{1}{2}}$ as described in Section 4. Then, for $(x,y)\in G_{hR}$, the analysis of the last two paragraphs can be repeated with the range of integration changed as indicated. Clearly the functions ϕ and ψ of (7.39) are analytic in x for (x,y) in G_{hR} and belong to their respective classes on $\bar{G}_{hR}$ and the function ϕ^* of (7.40) has the same property on the union of G_{hR}, its reflection in $y=0$, and the set $y=0$, $x\in B_{hR}$. Thus the second part of Theorem 7.3 follows.

We can now prove Theorem A′ as stated in Section 5. We construct $P_{R0}(f)$ as follows: Letting (r, σ) be polar coordinates, $0 \leqq r \leqq R$ and σ on the upper unit hemisphere, we define $f^*_j(r, \sigma) = f_j(r, \sigma)$ on the range above, $f^*_j(r, \sigma) = 0$ for $r \leqq 0$, and

$$f^*_j(r, \sigma) = \sum_{q=1}^{s-s_j+1} C_{s-s_j, q} f^*[R - q(r - R)], \qquad r \geqq \mathrm{R},$$

where the C's are determined by the conditions that

$$\sum_{q=1}^{h+1} C_{hq} \cdot (-q)^p = 1, \qquad 0 \leqq p \leqq h.$$

Then $f^*_j \in C^{s-s_j+\mu}$ on E^+ and vanishes outside G_{2R} with $\| f^* \|_{2R} \leqq Z_1(\mu, s_j) \cdot \| f \|$. We let U_R be defined by (7.36) with f_l replaced by f^*_l, let $P_R{}^k$ be the polynomial of degree $s + s_k$ such that $\nabla^p P_R{}^k(0, 0) = \nabla^p U_R{}^k(0, 0)$ for $0 \leqq p \leqq s + s_k$, and let

$$P_{R0}(f) = u_R \text{ where } u_R{}^k = U_R{}^k - P_R{}^k.$$

Then, clearly $u \in E_{R0}$, $\| u \| \leqq K_q(\mu) \cdot \| f \|$, and it is seen as in Part I that u is a solution of (5.11). Theorem B′ follows from the second part of Theorem 7.3.

To prove Theorem C′, let $H_R \in E_{R0}$ on $\bar{G}_R$ and be a solution of the homogeneous equations (5.11) on G_R. Let H^*_R be its extension as above, let

$$f^*_{jR} = L_{jk} H^*_R, \qquad U^*_R = P_{R0}(f^*_R), \qquad \mathfrak{H}_R = H^*_R - U^*_R.$$

Then U^*_R, H^*_R, and $\mathfrak{H}_R \in E_{2R0}$ with

$$\| U^*_R \|_{2R} \leqq Z_2 \| H_R \|_R, \qquad \| \mathfrak{H}_R \|_{2R} \leqq Z_3 \| H_R \|_R, \qquad \| H^*_R \|_{2R} \leqq Z_4 \| H_R \|_R$$

and $\mathfrak{H}_R$ is a solution of the homogeneous equations (5.11) on G_{2R}. By applying (7.31) with $u = \mathfrak{H}_R$, $a = 2R$, we obtain

$$(7.44) \qquad \mathfrak{H}_R{}^l(X) = -\int_{\Sigma_{2R}} B^\alpha[G^l(X, \Xi), \mathfrak{H}_R(\Xi)] n_\alpha \, dS_\Xi, \qquad X \in G_{2R}$$

since $\mathfrak{H}_R{}^k(\Xi)$ and $G^{lj}(X, \Xi)$ both have 0 Dirichlet data on $\eta = 0$ (see (7.29)). Clearly $\mathfrak{H}_R{}^l(X)$ can be extended analytically in x (X in fact) to any $G_{h, 2R} \supset G_{hR}$ with $0 < h \leqq h_1$. Now any derivative $D^{s+s_l+1} \mathfrak{H}_R{}^l(X)$ for $X \in G_{hR}$, $0 < h \leqq h_1$, is seen to be a linear combination of terms of the form

$$(7.45) \qquad I = \int_{\Sigma_{2R}} D_X{}^{s+s_l+1} D_\Xi{}^p G^{lj}(X, \Xi) D_\Xi{}^q \mathfrak{H}_R{}^k(\Xi) n_\alpha \, dS_\Xi,$$

$$p + q = s_j + s_k - 1.$$

The term (7.45) may be written in the form

$$I=\int_{\Sigma_{2R}} G(X,\Xi)\,[\phi(\Xi)-\sum_{w=0}^{h}\nabla^{w}\lambda(X_1)\cdot(\Xi-X_1)^{w}/w\,!]\,n_\alpha\,dS_{\Xi}$$

$$+\sum_{w=0}^{h}[\nabla^{w}\phi(X_1)\int_{\Sigma} G(X,\Xi)\,(\Xi-X_1)^{w}n_\alpha\,dS_{\Xi}]/w\,!,$$

$$(h=s-s_j+1+p),\ X=X_1+iX_2\in G_{hR},$$

where it is clear what G and ϕ stand for. Now, by using only the facts (derivable from homogeneity, etc. and $\mathcal{H}_R\in E_{2R,0}$) that

$$|\,G(X,\Xi)\,|\leqq Z_1\cdot\|\,\Xi-X\,\|^{s_j-s-\nu-2},\quad R\leqq|\,\Xi-X_1\,|\leqq\|\,\Xi-X\,\|;$$

$$|\,\nabla^{w}\phi(X_1)\,|\leqq\|\,\mathcal{H}_R\,\|_{2R}\cdot R^{s-s_j+p+1-w+\mu},$$

we find that

$$|\,\nabla^{s+s_l+1}\mathcal{H}_R{}^{l}(X)\,|\leqq Z_2(h,\mu,\nu,N,s_j,m_2,M)\cdot\|\,H_R\,\|_R\cdot R^{\mu-1},\qquad X\in G_{hR}$$

from which Theorem C′ follows easily since $\|\,H^*_R\,\|^*_R$ is also $\leqq Z_3\cdot\|\,H_R\,\|_R$ by Theorem 7.3 since $f^*=0$ on G_R.

UNIVERSITY OF CALIFORNIA.

REFERENCES.

[1] A. Friedman, "Classes of solutions of linear non-hyperbolic differential equations," to appear in *Journal of Mathematics and Mechanics.*

[2] P. Lax and A. N. Milgram, "Parabolic equations," *Annals of Mathematics Studies*, no. 33, Princeton University Press (1954), pp. 167-190.

[3] S. Mandelbrojt, *Séries de Fourier et classes quasi-analytiques de fonctions*, Collection Borel, Paris, 1935.

[4] C. B. Morrey, Jr., "On the analyticity of the solutions of analytic non-linear elliptic systems of partial differential equations, I," *American Journal of Mathematics*, vol. 80 (1958), pp. 198-218.

[5] L. Nirenberg, "Remarks on strongly elliptic partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 648-674.

REMARKS ON MY PAPER "THE JACOBIAN VARIETY OF AN ALGEBRAIC CURVE."*

By Wei-Liang Chow.

We should like to make two remarks on this paper, which was published in vol. 76 (1954), pp. 453-76, of this Journal.

(1) In section 5, at the bottom of p. 469, we have stated that if $\mathfrak{P}$ is a divisor class of degree $n > 2g$, rational over an extension K of k, and if $(x^1), \cdots, (x^n)$ are the n points contained in a generic positive divisor $\mathfrak{p}$ of $\mathfrak{P}$ over K, then all the n points $(x^1), \cdots, (x^n)$ are generic points of $\mathfrak{C}$ over K, distinct from each other, and any $n-g$ of these n points are independent with respect to each other over K and determine the remaining g points uniquely. On the basis of this statement it can be easily deduced that there is an automorphism of the field $K((x^1), \cdots, (x^n))$ over the field K which carries any set of $n-g$ of the n points $(x^1), \cdots, (x^n)$ into any other such set; furthermore, it is clear that such an automorphism over K is also an automorphism over $K((p))$, so that the Galois group of $K((x^1)), \cdots, (x^n))$ over $K((p))$ is $(n-g)$-fold transitive. Professor J. Igusa has kindly pointed out to us that it is by no means obvious that any $n-g$ points among the n points $(x^1), \cdots, (x^n)$ are independent with respect to each other over K, and that a formal proof of this statement is desirable, although it is sufficient for the purpose we had there to prove this for the special case where $\mathfrak{p}$ is a generic positive divisor of degree n over k in $\mathfrak{C}$, in which case the proof follows easily from the fact that the Galois group of $k((x^1), \cdots, (x^n))$ over $k((p))$ is the entire symmetric group of permutations of the n points $(x^1), \cdots, (x^n)$. We shall give here a simple proof of our statement as follows.

For any point (η) in $\mathfrak{C}$, we denote by $\mathfrak{C}^n(\eta)$ the subset in $\mathfrak{C}^n$ consisting of all points which represent positive divisors of degree n in $\mathfrak{C}$ having the point (η) as a component. It is clear that $\mathfrak{C}^n(\eta)$ is a subvariety of dimension $n-1$ in $\mathfrak{C}^n$, defined over $k((\eta))$; in fact, if (q) is the point in $\mathfrak{C}^n$ which represents the divisor consisting of the point (η) and $n-1$ independent generic points of $\mathfrak{C}$ over $k((\eta))$, then $\mathfrak{C}^n(\eta)$ is the locus of (q)

---

* Received December 1, 1957.

over $k((\eta))$. Furthermore, it is easily seen that if (x) is a generic point of $\mathfrak{C}$ over k, then $\mathfrak{C}^n(\eta)$ is the unique specialization of $\mathfrak{C}^n(x)$ over the specialization $(x) \rightarrow (\eta)$ over k. In order to prove our statement, it is sufficient to show that if the $n-g$ points $(x^1), \cdots, (x^{n-g})$ in $\mathfrak{p}$ are independent generic points of $\mathfrak{C}$ over K, then the same is true for the $n-g$ points $(x^1), \cdots, (x^{n-g-1})$, (x^s), for any choice of the point (x^s) among the remaining g points in $\mathfrak{p}$ (always under the assumption $n > 2g$). To show this, we shall assume that it is possible to choose the point (x^s) so that it is algebraic over $K((x^1), \cdots, (x^{n-g-1}))$, and we shall show that this leads to a contradiction. Since $(x^1), \cdots, (x^{n-g-1})$ are independent generic points of $\mathfrak{C}$ over K, the set of all positive divisor in the residual class of $\mathfrak{P}$ with respect to the divisor $\sum_{i=1}^{n-g-1}(x^i)$ is a complete linear system of dimension 1, rational over $K((x^1), \cdots, (x^{n-g-1}))$, and hence is represented in $\mathfrak{C}^{g+1}$ by a subvariety $\mathfrak{E}$ of dimension 1, defined over $K((x^1), \cdots, (x^{n-g-1}))$. The assumption that (x^s) is algebraic over $K((x^1), \cdots, (x^{n-g-1}))$ implies that (x^s) is a fixed point of this complete linear system, so that we have the relation $\mathfrak{E} \subset \mathfrak{C}^{g+1}(x^s)$. Consider now the simultaneous specialization $(x^i) \rightarrow (x^{n-i+1})$, for $i = 1, \cdots, n-g-1$, over K, and let $\mathfrak{E}'$ and (ξ) be specializations of the positive 1-cycle $\mathfrak{E}$ and the point (x^s) over this specialization over K; then every component $\mathfrak{E}_0'$ in $\mathfrak{E}'$ is a subvariety of dimension 1 and we have the relation $\mathfrak{E}_0' \subset \mathfrak{C}^{g+1}(\xi)$. If (q) is any point in $\mathfrak{E}_0'$ and $\mathfrak{q}$ is the positive divisor in $\mathfrak{C}$ represented by (q), then the positive divisor $\mathfrak{q} + \sum_{i=1}^{n-g-1}(x^{n-i+1})$ is a specialization over K of a positive divisor in $\mathfrak{P}$ and hence is contained in $\mathfrak{P}$; it follows that every such positive divisor $\mathfrak{q}$ is an element in the residual class of $\mathfrak{P}$ with respect to the divisor $\sum_{i=1}^{n-g-1}(x^{n-i+1})$. Now, the set of all positive divisors in this last mentioned residual class is the complete linear system determined by the positive divisor $\sum_{i=1}^{g+1}(x^i)$ and since $n-g \geqq g+1$, the points $(x^1), \cdots, (x^{g+1})$ are independent generic points of $\mathfrak{C}$ over K, and hence the divisor $\sum_{i=1}^{g+1}(x^i)$ is a generic positive divisor of degree $g+1$ over K in $\mathfrak{C}$. This implies in particular that this complete linear system has the dimension 1 and hence is represented in $\mathfrak{C}^{g+1}$ by a subvariety $\mathfrak{E}''$ of dimension 1; since $\mathfrak{E}_0' \subset \mathfrak{E}''$ and both varieties have the same dimension, we conclude that $\mathfrak{E}_0' = \mathfrak{E}''$ and hence $\mathfrak{E}'' \subset \mathfrak{C}^{g+1}(\xi)$. This means that the complete linear system determined by the generic positive divisor $\sum_{i=1}^{g+1}(x^i)$ of degree $g+1$ over K in $\mathfrak{C}$ has a fixed point, which is evidently impossible.

(2) In the last paragraph of our paper, on p. 475, we have given a proof of the statement that if the curve $\mathfrak{C}$ contains a rational divisor $\mathfrak{o}$ over k of degree 1, then every rationally defined divisor class over any extension K of k is also rational over K. Dr. P. Roquette has kindly called our attention to the fact that the proof given there holds only for the case where $\mathfrak{o}$ is a positive divisor, or rather a prime divisor, so that there is in this sense a gap in our proof. However, this gap can be easily remedied as follows. In fact, it is sufficient to prove the following statement: If $\mathfrak{C}$ contains a rational positive divisor $\mathfrak{o}$ over k of degree s and if $\mathfrak{P}$ is a rationally defined divisor class over K, then the divisor class $s\mathfrak{P}$ is rational over K. Now, if $(x^1), \cdots, (x^s)$ are the s points (which need not be distinct) contained in $\mathfrak{o}$, then, by what we have proved there, there exists a rational divisor $\mathfrak{p}_i$ over $K((x^i))$ in $\mathfrak{P}$ for each $i = 1, \cdots, s$; the divisor $\sum_{i=1}^{s} \mathfrak{p}_i$ is evidently rational over K and is contained in sP.

THE JOHNS HOPKINS UNIVERSITY.

CENTRAL LIBRARY
UNIVERSITY

SPHERICAL FUNCTIONS ON A SEMISIMPLE LIE GROUP, I.*

By HARISH-CHANDRA.[1]

1. Introduction. Let G be a connected semisimple Lie group with finite center and K a maximal compact subgroup of G. A complex-valued function f on G is called a spherical function if $f(k_1 x k_2) = f(x)$ for $k_1, k_2 \in K$ and $x \in G$. Let dk denote the normalized Haar measure of K. A spherical function $f \neq 0$ is said to be elementary (see Godement [4, p. 497]) if it is continuous and if

$$\int_K f(xky)\, dk = f(x) f(y)$$

for x, y in G. It can be shown that every such function is analytic and, in fact, it is possible to give an alternative characterization of elementary spherical functions as follows. Let $\mathfrak{Z}$ be the algebra of all differential operators on G which are invariant under left translations by elements of G and right translations by elements of K. Then a spherical function f of class C^∞ is elementary if and only if $f(1) = 1$ and f is an eigenfunction of every differential operator in $\mathfrak{Z}$. Finally, there exists a simple integral formula (see [5(d), Theorem 5]) for any such function.

It follows from the Plancherel formula for the factor space G/K (see [5(m), p. 204]) that an "arbitrary" spherical function can be "expanded" in terms of the elementary ones. However the fundamental measure appearing in this formula had, so far, not been satisfactorily related to the group structure of G. If we agree to ignore certain technical complications, the situation may roughly be described as follows. A certain class of elementary spherical functions (of positive-definite type) can be parameterized by a space E/W. Here E is a finite-dimensional real Euclidean space, W is a finite group of linear transformations in E and E/W denotes the quotient space obtained by identifying points in E which are congruent under W. Let ϕ_λ denote the elementary spherical function which corresponds to a point $\lambda \in E$ so that $\phi_{s\lambda} = \phi_\lambda$ $(s \in W)$. For any continuous spherical function f with compact support, put

$$\bar{f}(\lambda) = \int f(x) \phi_\lambda(x^{-1})\, dx$$

---

* Received July 16, 1957.

[1] John Simon Guggenheim Fellow.

where dx is the Haar measure of G. Then the Plancherel formula asserts[2] the existence of a unique positive measure $d\mu$ on E (which is invariant under W) such that

$$\int |f(x)|^2\,dx = \int |\bar{f}(\lambda)|^2\,d\mu$$

for all such f. The problem is to determine this measure $d\mu$. Let $d\lambda$ denote the Euclidean measure on E. In this paper we shall give an asymptotic expansion for ϕ_λ on G. The leading terms of this expansion involve a certain coefficient $\boldsymbol{c}(\lambda)$, which, considered as a function of λ, is analytic on E except on certain hyperplanes (see Lemmas 37 and 52). In any case, the reciprocal $\boldsymbol{c}^{-1}$ is analytic on E and it will be shown in another paper that[3] $d\mu = |\boldsymbol{c}(\lambda)|^{-2}\,d\lambda$ (if dx and $d\lambda$ are suitably normalized). On the other hand the Fourier transform[2] of $\boldsymbol{c}$ is a distribution on E which is given by a simple formula in which the group structure of G enters in a very direct manner (see Theorem 5).

The above outline shows that our problem can be divided into three more or less distinct parts: (1) the asymptotic formula for ϕ_λ, (2) the investigation of the function $\boldsymbol{c}$ and (3) the proof of the relation $d\mu = |\boldsymbol{c}(\lambda)|^{-2}\,d\lambda$. Only the first two of these questions will be taken up in this paper. For (1) we consider the system of differential equations $D\phi_\lambda = \chi_\lambda(D)\phi_\lambda$ $(D \in \mathfrak{Z})$ where $\chi_\lambda(D)$ is the eigenvalue corresponding to the operator D. Actually the equation $\omega\phi_\lambda = \chi_\lambda(\omega)\phi_\lambda$, corresponding to the Casimir operator ω, plays a predominant role in this discussion. In fact, this single equation, together with some general properties of ϕ_λ, permits us to derive the asymptotic formula for ϕ_λ.

Now in order to obtain more information about $\boldsymbol{c}$, we have to investigate ϕ_λ as a function of λ, in the neighborhood of infinity on G. It turns out that one can select a polynomial function π on E such that $\boldsymbol{b} = \pi\boldsymbol{c}$ is everywhere analytic on E. Moreover every derivative of $\boldsymbol{b}$ is majorized on E by a suitable polynomial function. We shall see in another paper that $|\boldsymbol{b}(s\lambda)| = |\boldsymbol{b}(\lambda)|$ for $s \in W$.

The contents of this paper are as follows. In Section 2 we collect some elementary facts which are obtained by considering the finite-dimensional representations of G. Section 3 is devoted to deriving the consequences of two unpublished lemmas of Chevalley. These results, which are of an algebraic nature, will be used constantly during this and the next paper of this series. In Section 4 we define a homomorphism γ of $\mathfrak{J}$ onto the algebra J consisting of those polynomial functions on E which are invariant under W. Let l be the rank of symmetric Riemannian space G/K. Then it is possible to select a connected abelian Lie subgroup $A_{\mathfrak{p}}$ of G of dimension l such that $G = KA_{\mathfrak{p}}K$. Obviously a spherical function f is completely determined by its restriction $\bar{f}$ on $A_{\mathfrak{p}}$. In Sections 5 and 6 we investigate the relationship[4] between $\overline{Df}$ and $\bar{f}$ for any $D \in \mathfrak{J}$. It turns out that one can define a differential operator $\delta'(D)$ on an open dense subset $A_{\mathfrak{p}}'$ of $A_{\mathfrak{p}}$ such that $\overline{Df} = \delta'(D)\bar{f}$ on $A_{\mathfrak{p}}$. Moreover there is an intimate connection between $\delta'(D)$ and $\gamma(D)$ and this permits us to prove (see the corollary of Theorem 2) that if w is the order of the group W, there cannot exist more than w linearly independent analytic functions on any open connected subset of $A_{\mathfrak{p}}'$, which are all eigenfunctions of $\delta'(D)$ with the same eigenvalues, for every $D \in \mathfrak{J}$. Therefore if we could somehow find w such functions, corresponding to the eigenvalues $\chi_\lambda(D)$, on a connected component $A_{\mathfrak{p}}^+$ of $A_{\mathfrak{p}}'$, ϕ_λ would be expressible on $A_{\mathfrak{p}}^+$ as a linear combination of these. In order to do this we compute the operator $\delta'(\omega)$ and, starting from the equation $\delta'(\omega)\phi = \chi_\lambda(\omega)\phi$, give a method of constructing the required functions $\phi_\lambda^{(i)}$ $(1 \leqq i \leqq w)$. The asymptotic behaviour of the $\phi_\lambda^{(i)}$ is obvious from their construction and so in this way, we get an asymptotic formula for ϕ_λ on $A_{\mathfrak{p}}^+$.

---

[2] This is a simplified version of the true picture and therefore is not entirely accurate.

[3] This is reminiscent of a result of Weyl [8(a), p. 266] on ordinary differential equations.

In order to make further progress, it is necessary to make a closer study of the function ϕ_0 corresponding to $\lambda = 0$. Theorem 3 contains the main result on ϕ_0. It is possible to derive from this certain important consequences (see Lemma 45 and Theorems 4 and 5) and actually to obtain explicit formulae for $\boldsymbol{c}$ and its Fourier transform. Section 12 is devoted to a deeper study of the function $\boldsymbol{c}$ and the principal result is given in Lemma 52. In Section 13, we give some explicit calculations for the case $l = 1$. These will be required in the next paper of this series. The case when G is complex is especially simple and therefore it is discussed separately in Section 14. Certain simple lemmas in analysis, which are often needed during this paper, are collected together in the Appendix (§ 15).

Some of the results of this paper have been announced in a short note [5(n)].

2. Preliminary lemmas. Let R and C be the fields of real and complex numbers respectively and G a connected semisimple Lie group and $\mathfrak{g}_0$ its Lie algebra over R. Define $\mathfrak{k}_0$ and $\mathfrak{p}_0$ as usual (see [5(c), p. 187]) and let K be the analytic subgroup of G corresponding to $\mathfrak{k}_0$. Since K contains the center of G (see [7]) and since we shall be concerned in this paper primarily with functions on G/K, G can be replaced by any connected group locally isomorphic to it. Let G_C be a simply connected complex-analytic group corresponding to the complexification $\mathfrak{g}$ of $\mathfrak{g}_0$. Then we may assume that G is the real analytic subgroup of G_C which corresponds to $\mathfrak{g}_0$. This permits us to identify the finite-dimensional representations of G with those of $\mathfrak{g}_0$ and thus also with the complex representations of G_C and $\mathfrak{g}$. If π is such a representation on a vector space V, one can always introduce the structure of a Hilbert space in V in such a way that $\pi(X)$ becomes skew-Hermitian for $X \in \mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$. We shall always tacitly assume that such a structure has been defined. Also observe that K is now compact.

---

[4] The results of Sections 5 and 6 should be compared with Theorem 1 of [5(k)].

Let $\mathfrak{h}_{\mathfrak{p}_0}$ be a maximal abelian subspace of $\mathfrak{p}_0$ and $\mathfrak{h}_0$ a Cartan subalgebra of $\mathfrak{g}_0$ containing $\mathfrak{h}_{\mathfrak{p}_0}$. Then $\mathfrak{h}_0 = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{h}_{\mathfrak{k}_0}$ where $\mathfrak{h}_{\mathfrak{k}_0} = \mathfrak{h}_0 \cap \mathfrak{k}_0$. Complexify $\mathfrak{k}_0$, $\mathfrak{p}_0$, $\mathfrak{h}_0$, $\mathfrak{h}_{\mathfrak{p}_0}$, $\mathfrak{h}_{\mathfrak{k}_0}$ to $\mathfrak{k}$, $\mathfrak{p}$, $\mathfrak{h}$, $\mathfrak{h}_{\mathfrak{p}}$, $\mathfrak{h}_{\mathfrak{k}}$ respectively in $\mathfrak{g}$ and introduce compatible orders (see [4(1), § 2]) in the spaces of real-valued linear functions on $\mathfrak{h}_{\mathfrak{p}_0} + (-1)^{\frac{1}{2}}\mathfrak{h}_{\mathfrak{k}_0}$ and $\mathfrak{h}_{\mathfrak{p}_0}$. Let P denote the set of all positive roots of $\mathfrak{g}$ (with respect to $\mathfrak{h}$) under this order. Consider the set Σ of all linear functions $\lambda \neq 0$ on $\mathfrak{h}_{\mathfrak{p}}$ which are restrictions of some α in P. Then every element in Σ is positive under the above order.

LEMMA 1. *Let π be an irreducible finite-dimensional representation of $\mathfrak{g}$ such that the zero representation of $\mathfrak{k}$ occurs in the reduction*[5] *of π with respect to $\mathfrak{k}$. Then if λ is the highest weight of π, λ is identically zero on $\mathfrak{h}_{\mathfrak{k}}$.*

Let $\psi_0 \neq 0$ be a vector in the representation space V belonging to the weight λ. For any root α, define X_α as usual (see [5(c), p. 188]) and put $\mathfrak{n} = \sum_{\alpha \in P_+} CX_\alpha$ where P_+ is the set of those roots $\alpha \in P$ whose restriction on $\mathfrak{h}_{\mathfrak{p}}$ is not zero. Let $A_{\mathfrak{p}}$ and N be the analytic subgroups of G corresponding to $\mathfrak{h}_{\mathfrak{p}_0}$ and $\mathfrak{n}_0 = \mathfrak{n} \cap \mathfrak{g}_0$ respectively. Then $G = KA_{\mathfrak{p}}N$ (see Iwasawa [6]). It is clear that $\pi(n)\psi_0 = \psi_0$ for $n \in N$ and therefore the vector space $C\psi_0$ is invariant under $\pi(A_{\mathfrak{p}}N)$. Hence V is spanned by vectors of the form $\pi(k)\psi_0$ $(k \in K)$. Put $E = \int_K \pi(k)\,dk$ where dk is the normalized Haar measure of K. Then it follows that $EV = CE\psi_0$. Now we can, by hypothesis, select a unit vector ψ in V which is invariant under K. Then $\psi = E\psi = cE\psi_0$ where $c \in C$. But $\pi(X)E = E\pi(X) = 0$ if $X \in \mathfrak{k}$ and therefore $\lambda(H)E\psi_0 = E\pi(H)\psi_0 = 0$ for $H \in \mathfrak{h}_{\mathfrak{k}}$. Since $\psi \neq 0$, this implies that $\lambda(H) = 0$.

---

[5] It follows from Lemmas 2 and 3 of [5(c)] that $\pi(\mathfrak{k})$ is fully reducible.

It is well known that the exponential mapping is univalent and regular on $\mathfrak{p}_0$. Hence $A_{\mathfrak{p}}$ is simply connected and, for any $x \in G$, there exists a unique element $H(x) \in \mathfrak{h}_{\mathfrak{p}_0}$ such that $x \in K(\exp H(x))N$ (see [6]). Moreover $x \to H(x)$ is an analytic mapping of G into $\mathfrak{h}_{\mathfrak{p}_0}$ (see [5(c), Lemma 26]).

Let $\mathfrak{F}_0$ denotes the set of all linear functions λ of $\mathfrak{h}_{\mathfrak{p}}$ with the property that there exists a representation π of $\mathfrak{g}$ satisfying the conditions of Lemma 1, whose highest weight coincides on $\mathfrak{h}_{\mathfrak{p}}$ with λ.

LEMMA 2. *Let Λ be the highest weight of any irreducible finite-dimensional representation π of $\mathfrak{g}$ and let λ denote the restriction of Λ on $\mathfrak{h}_{\mathfrak{p}}$. Then $2\lambda \in \mathfrak{F}_0$.*

Select a unit vector ψ in the representation space V belonging to the weight Λ and put[6]

$$\phi(x) = \int_K |\pi(xk)\psi|^2 \, dk \qquad (x \in G).$$

Since $\pi(k)$ is unitary $(k \in K)$ and $\pi(n)\psi = \psi$ $(n \in N)$, it is clear that $|\pi(x)\psi| = e^{\Lambda(H(x))}$. Hence $\phi(x) = \int_K e^{2\Lambda(H(xk))} dk$. Also it follows from its definition that ϕ is spherical, that is, $\phi(k_1 x k_2) = \phi(x)$ $(k_1, k_2 \in K; x \in G)$. Let ϕ_y $(y \in G)$ denote the right translate of ϕ by y so that $\phi_y(x) = \phi(xy)$ $(x \in G)$. Select an orthonormal base $\psi_0 = \psi, \psi_1, \cdots, \psi_r$ for V and let $\pi(x)\psi_i = \sum_{0 \leqq j \leqq r} \psi_j a_{ji}(x)$ $(0 \leqq i \leqq r)$ where a_{ji} are analytic functions on G. Then

$$\pi(xk)\psi = \sum_j \psi_j a_j(xk) = \sum_{j,i} \psi_j a_{ji}(x) a_i(k)$$

where $a_i = a_{i0}$. Therefore

$$|\pi(xk)\psi|^2 = \sum_j |\sum_i a_{ji}(x) a_i(k)|^2$$

and[7]

$$\phi(x) = \sum_{0 \leqq i,j,m \leqq r} a_{ji}(x)(\operatorname{conj} a_{jm}(x)) c_{im} \qquad (x \in G)$$

where c_{im} are certain constants. Let U' be the linear space spanned over C by the $(r+1)^2$ functions $\sum_{0 \leqq j \leqq r} a_{ji}(\operatorname{conj} a_{jm})$ $(0 \leqq i, m \leqq r)$. Then it is clear that $\phi_y \in U'$. Let U be the subspace of U' spanned by all ϕ_y $(y \in G)$. We define a representation τ of G on U as follows. If $\phi' \in U$, $\tau(y)\phi'$ is the function $x \to \phi'(xy)$ on G. It is clear that $\tau(k)\phi = \phi_k = \phi$ $(k \in K)$. Moreover $\phi \neq 0$ since $\phi(1) = 1$ and therefore the trivial representation of K

---

[6] We denote the scalar product of two elements ϕ_1, ϕ_2 in V in the usual way by (ϕ_1, ϕ_2). Similarly $|\phi_1|$ denotes the norm of ϕ_1.

[7] conj c denotes the conjugate of a complex number c.

occurs in the reduction of τ. Also as we shall see below (corollary to Lemma 3), τ is irreducible.

Now we may obviously assume that each ψ_i belongs to a weight Λ_i $(0 \leqq i \leqq r,\ \Lambda_0 = \Lambda)$ of π. Then $a_{ji}(x \exp H) = a_{ji}(x) e^{\Lambda_i(H)}$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$. Moreover the weights being real[8] linear functions,

$$\sum_j a_{ji}(xh) \operatorname{conj} a_{jm}(xh) = \sum_j a_{ji}(x)(\operatorname{conj} a_{jm}(x)) \exp\{\Lambda_i(H) + \Lambda_m(H)\}$$

where $h = \exp H$ $(x \in G, H \in \mathfrak{h}_{\mathfrak{p}_0})$. Let μ be the highest weight of τ. Then we conclude from the above formula that μ coincides on $\mathfrak{h}_{\mathfrak{p}_0}$ with $\Lambda_i + \Lambda_m$ for some i and m. Since $\Lambda_i + \Lambda_m \leqq 2\Lambda_0 = 2\Lambda$, it follows from the compatibility of our orders that $\bar{\mu} \leqq 2\lambda$, where $\bar{\mu}$ is the restriction of μ on $\mathfrak{h}_{\mathfrak{p}}$. On the other hand[6]

$$\begin{aligned}\phi(x) &= \int_K |\pi(xk)\psi|^2\, dk \\ &= \sum_{0 \leqq i,j,m \leqq r} a_{ji}(x)(\operatorname{conj} a_{jm}(x)) \int_K (\psi_i, \pi(k)\psi) \operatorname{conj}(\psi_m, \pi(k)\psi)\, dk.\end{aligned}$$

Now[9] $a_{ji}(\exp H) = \delta_{ji} e^{\Lambda_j(H)}$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$. Hence $\phi(\exp H) = \sum_{0 \leqq i \leqq r} e^{2\Lambda_i(H)} c_i$ where

$$c_i = \int_K |(\psi_i, \pi(k)\psi)|^2\, dk \geqq 0.$$

Let $f_0, f_1, \cdots, f_p$ be a base for U over C such that each f_i belongs to a weight μ_i of the representation τ and $\mu_0 = \mu$. Then $\phi = \sum_{0 \leqq i \leqq p} b_i f_i$ $(b_i \in C)$ and therefore

$$\tau(\exp H)\phi = \sum_{0 \leqq i \leqq p} b_i e^{\mu_i(H)} f_i \qquad (H \in \mathfrak{h}_{\mathfrak{p}_0}).$$

This shows that $\phi(\exp H) = \sum_i b_i f_i(1) e^{\mu_i(H)}$. Let $\bar{\mu}_i$ denote the restriction of μ_i on $\mathfrak{h}_{\mathfrak{p}}$. Then if we note that

$$c_0 = \int |(\psi, \pi(k)\psi)|^2\, dk > 0$$

and recall that the exponentials of distinct linear functions on $\mathfrak{h}_{\mathfrak{p}}$ are linearly independent over C (see [5(b), Lemma 41]), it follows from a comparison of the above two formulas for $\phi(\exp H)$ that $2\lambda = \bar{\mu}_i$ for some i. But $\mu \geqq \mu_i$ and therefore $\bar{\mu} \geqq \bar{\mu}_i = 2\lambda$. However we have seen above that $\bar{\mu} \leqq 2\lambda$ and so $\bar{\mu} = 2\lambda$. This proves Lemma 2.

---

[8] A linear function on $\mathfrak{h}$ or $\mathfrak{h}_{\mathfrak{p}}$ is said to be real, if it takes only real values on $\mathfrak{h}_{\mathfrak{p}_0} + (-1)^{\frac{1}{2}}\mathfrak{h}_{\mathfrak{k}_0}$ or $\mathfrak{h}_{\mathfrak{p}_0}$ respectively.

[9] As usual $\delta_{ij} = 1$ or 0 according as $i = j$ or not. Sometimes it will be convenient to write $\delta_i{}^j$ instead of δ_{ij}.

Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$. We regard elements of $\mathfrak{B}$ as left-invariant differential operators on G (see [5(g), § 4]). From now on we shall make use of the notational conventions described in footnote 1 of [5(k)]. Define $\mathfrak{n} = \sum_{\alpha \in P_+} CX_\alpha$ as before and let $\mathfrak{H}_\mathfrak{p}$ be the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{h}_\mathfrak{p})$. We denote the centralizer of $\mathfrak{k}$ in $\mathfrak{B}$ by $I_\mathfrak{g}$.

LEMMA 3. *For any $b \in \mathfrak{B}$, there exists a unique element $u_b \in \mathfrak{H}_\mathfrak{p}$ such that $b - u_b \in \mathfrak{k}\mathfrak{B} + \mathfrak{B}\mathfrak{n}$. The degree of u_b does not exceed that of b. Moreover if ν is any linear function on $\mathfrak{h}_\mathfrak{p}$ and*

$$g(x) = \int_K e^{\nu(H(xk))} dk \qquad (x \in G),$$

then $qg = \chi_\nu(u_q) g$ for $q \in I_\mathfrak{g}$. Here χ_ν is the homomorphism of $\mathfrak{H}_\mathfrak{p}$ into C such that $\chi_\nu(1) = 1$ and $\chi_\nu(H) = \nu(H)$ $(H \in \mathfrak{h}_\mathfrak{p})$.

In order to prove the first statement, it is sufficient to show that $\mathfrak{B}$ is the direct sum of $\mathfrak{H}_\mathfrak{p}$ and $\mathfrak{k}\mathfrak{B} + \mathfrak{B}\mathfrak{n}$. Let $\mathfrak{X}$ and $\mathfrak{N}$ be the subalgebras of $\mathfrak{B}$ generated by $(1, \mathfrak{k})$ and $(1, \mathfrak{n})$ respectively. Consider the linear mapping of the tensor product $\mathfrak{X} \times \mathfrak{H}_\mathfrak{p} \times \mathfrak{N}$ into $\mathfrak{B}$ which maps $x \times h \times n$ onto xhn $(x \in \mathfrak{X}, h \in \mathfrak{H}_\mathfrak{p}, n \in \mathfrak{N})$. Then our first two assertions follow immediately from Lemma 12 of [5(c)] if we recall that $\mathfrak{g}$ is the direct sum of $\mathfrak{k}$, $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{n}$.

Now it is obvious from the definition of $H(x)$ that $H(xn) = H(x)$ $(n \in N)$ and[10] $H(xh) = H(x) + \log h$ $(h \in A_\mathfrak{p})$. Therefore if $F(x) = e^{\nu(H(x))}$ $(x \in G)$, it follows that $F(x; b) = 0$ for $b \in \mathfrak{B}\mathfrak{n}$ and $F(x; u) = \chi_\nu(u) F(x)$ $(u \in \mathfrak{H}_\mathfrak{p})$. Now put[11] $F(x : k) = F(xk)$ $(x \in G, k \in K)$. Then if $q \in I_\mathfrak{g}$, it is clear that $F(x; q : k) = F(xk; q)$. Hence

$$g(x; q) = \int_K F(x; q : k) dk = \int_K F(xk; q) dk.$$

But $q = b_1 + b_2 + u_q$ where $b_1 \in \mathfrak{k}\mathfrak{B}$ and $b_2 \in \mathfrak{B}\mathfrak{n}$. Hence

$$F(xk; q) = F(xk; b_1) + \chi_\nu(u_q) F(xk).$$

However if $b \in \mathfrak{B}$, it is obvious that $\int_K F(xkk_1; b) dk$ is actually independent of $k_1 \in K$. Therefore $\int F(xk; b') dk = 0$ for any $b' \in \mathfrak{k}\mathfrak{B}$ and hence

$$g(x; q) = \int_K F(xk; q) dk = \chi_\nu(u_q) \int_K F(xk) dk = \chi_\nu(u_q) g(x).$$

---

[10] $\log h$ denotes the unique element $H \in \mathfrak{h}_{\mathfrak{p}_0}$ such that $\exp H = h$.

[11] Here we follow the mode of writing introduced in [5(k), § 2].

COROLLARY. *The representation τ defined during the proof of Lemma 2 is irreducible.*

We denote the corresponding representation of $\mathfrak{B}$ on U also by τ. Then it is clear that $\tau(b)\phi' = b\phi'$ for any $\phi' \in U$ and $b \in \mathfrak{B}$. Hence U consists of functions of the form $b\phi$ $(b \in \mathfrak{B})$. Let E denote the projection $\int_K \tau(k)\,dk$. Then $EU = E\tau(\mathfrak{B})\phi$. However since $\tau(k)\phi = \phi$ $(k \in K)$, it follows that $Eb\phi = q\phi$ where[12] $q = \int_K b^k\,dk \in I_{\mathfrak{g}}$ $(b \in \mathfrak{B})$. But

$$\phi(x) = \int_K e^{2\Lambda(H(xk))}\,dk$$

and therefore $EU = C\phi$ from Lemma 3. Hence the trivial representation of K occurs exactly once in the reduction of U under $\tau(K)$. Now let U_1 be any subspace of U which is invariant and irreducible under τ and such that $EU_1 \neq \{0\}$. (It is obvious that such a space exists.) Then $\phi \in EU_1 \subset U_1$ and therefore $U = \tau(\mathfrak{B})\phi \subset U_1$. This proves that $U_1 = U$ and therefore U is irreducible.

LEMMA 4. *Suppose u is an element in $\mathfrak{H}_{\mathfrak{p}}$ such that $\chi_\lambda(u) = 0$ for all $\lambda \in \mathfrak{F}_0$. Then $u = 0$.*

Let $L = \dim \mathfrak{h}$. Then (see [5(b), Theorem 1]) there exist L linearly independent linear functions $\Lambda_1, \cdots, \Lambda_L$ on $\mathfrak{h}$ with the property that $m_1\Lambda_1 + \cdots + m_L\Lambda_L$ is the highest weight of an irreducible finite-dimensional representation of $\mathfrak{g}$ whenever $m_1, \cdots, m_L$ are nonnegative integers. Let λ_i denote the restriction of $2\Lambda_i$ on $\mathfrak{h}_{\mathfrak{p}}$. Then if $l = \dim \mathfrak{h}_{\mathfrak{p}}$, it is obvious that we can choose l linearly independent elements, say $\lambda_1, \cdots, \lambda_l$, among $\lambda_1, \cdots, \lambda_L$. Then if $m_1, \cdots, m_l$ are nonnegative integers, it follows from Lemma 2 that $m_1\lambda_1 + \cdots + m_l\lambda_l \in \mathfrak{F}_0$. Our assertion is now an immediate consequence of Lemma 32 of [5(b)].

LEMMA 5. *Let π be an irreducible representation of G on a finite-dimensional vector space V. Suppose ϕ is a unit vector in V such that $\pi(k)\phi = \phi$ for all $k \in K$. Then*

$$(\phi, \pi(x)\phi) = \int_K e^{\lambda(H(xk))}\,dk \qquad (x \in G)$$

where λ is the highest weight of π.

---

[12] For any $x \in G_c$, $b \to b^x$ $(b \in \mathfrak{B})$ denotes the automorphism of $\mathfrak{B}$ which coincides with $\mathrm{Ad}(x)$ on $\mathfrak{g}$.

Let ψ be a unit vector in V belonging to the weight λ. Since $G = KA_{\mathfrak{p}}N$, it is clear that V is spanned by vectors of the form $\pi(k)\psi$ $(k \in K)$. Put $E = \int_K \pi(k)\,dk$. Then $E\pi(k)\psi = E\psi$ and therefore $EV = CE\psi$. But $\phi = E\phi \in EV$ and so $\phi = cE\psi$ for some $c \in C$. It is obvious that E is self-adjoint and $E^2 = E$. Hence

$$(\phi, \pi(x)\phi) = |c|^2 (\psi, E\pi(x)E\psi) \qquad (x \in G).$$

Now let $k \in K$ and $x \in G$. Then $xk = k'(\exp H(xk))n$ where $k' \in K$ and $n \in N$. Hence

$$E\pi(xk)\psi = e^{\lambda(H(xk))}E\pi(k')\psi = e^{\lambda(H(xk))}E\psi.$$

Therefore

$$E\pi(x)E\psi = \int_K E\pi(xk)\psi\,dk = \int_K e^{\lambda(H(xk))}dk\,E\psi.$$

Since $|c|^2 |E\psi|^2 = |\phi|^2 = 1$, this implies that

$$(\phi, \pi(x)\phi) = |c|^2(\psi, E\pi(x)E\psi) = \int_K e^{\lambda(H(xk))}dk.$$

3. Some results of Chevalley and their consequences. Let M be the centralizer and M' the normalizer of $\mathfrak{h}_{\mathfrak{p}_0}$ in K. Then $W = M'/M$ is a finite group (see [5(j), p. 619]) which operates as a group of linear transformations on $\mathfrak{h}_{\mathfrak{p}}$ in the obvious way. This linear representation of W being faithful, we can identify W with the corresponding linear group. We shall call W the little Weyl group of $\mathfrak{g}_0$ with respect to[13] $\mathfrak{h}_{\mathfrak{p}_0}$.

Put $B(X,Y) = \mathrm{sp}(\mathrm{ad}\,X\,\mathrm{ad}\,Y)$ $(X, Y \in \mathfrak{g})$ where $X \to \mathrm{ad}\,X$ denotes the adjoint representation of $\mathfrak{g}$. Then the quadratic form $B(X,X)$ is positive-definite on $\mathfrak{p}_0$. Therefore it defines a Euclidean metric on $\mathfrak{p}_0$ and hence also on $\mathfrak{h}_{\mathfrak{p}_0}$. Define Σ as in the beginning of Section 2. Then for each $\alpha \in \Sigma$, there exists a unique element $H_\alpha \in \mathfrak{h}_{\mathfrak{p}_0}$ such that $B(H, H_\alpha) = \alpha(H)$ for every $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Let s_α denote the linear transformation in $\mathfrak{h}_{\mathfrak{p}_0}$ which corresponds to the reflexion in the hyperplane $\alpha = 0$. Then s_α is given by $s_\alpha H = H - 2\{\alpha(H)/\alpha(H_\alpha)\}H_\alpha$ $(H \in \mathfrak{h}_{\mathfrak{p}})$. It is known (see Cartan [2]) that $s_\alpha \in W$. The following lemma has been proved by Chevalley.[14]

LEMMA 6 (Chevalley). *Let H_0 be any element in $\mathfrak{h}_{\mathfrak{p}}$ and W' the sub-*

---

[13] It is seen without difficulty that $M'A_{\mathfrak{p}}$ and $MA_{\mathfrak{p}}$ respectively are the normalizer and centralizer of $\mathfrak{h}_{\mathfrak{p}_0}$ in G. Hence $W = M'A_{\mathfrak{p}}/MA_{\mathfrak{p}}$ is independent of our choice of $\mathfrak{k}_0$, so long as $\mathfrak{h}_{\mathfrak{p}_0}$ remains fixed.

[14] I am grateful to Professor Chevalley for showing me his unpublished results.

group consisting of those elements $s \in W$ which leave H_0 fixed. Then W' is generated by the reflexions s_α corresponding to those $\alpha \in \Sigma$ for which $\alpha(H_0) = 0$.

COROLLARY. *W is generated by s_α $(\alpha \in \Sigma)$.*

This follows by taking $H_0 = 0$. (This corollary had been verified by Cartan [2] in the case of classical Lie algebras.)

Let $S(\mathfrak{p})$ and $S(\mathfrak{h}_\mathfrak{p})$ denote the symmetric algebras over $\mathfrak{p}$ and $\mathfrak{h}_\mathfrak{p}$ respectively. Then $S(\mathfrak{p}) \supset S(\mathfrak{h}_\mathfrak{p})$ and we can identify them with the algebras of polynomial functions on $\mathfrak{p}$ and $\mathfrak{h}_\mathfrak{p}$ respectively by means of the non-degenerate bilinear form $B(X, Y)$ (see [5(k), p. 93]). Moreover $\mathrm{Ad}(k)\mathfrak{p} = \mathfrak{p}$ $(k \in K)$ and therefore K operates on $\mathfrak{p}$ and therefore also on $S(\mathfrak{p})$. Similarly W operates on $S(\mathfrak{h}_\mathfrak{p})$. Let $I(\mathfrak{p})$ and $I(\mathfrak{h}_\mathfrak{p})$ be the subalgebras consisting of those elements of $S(\mathfrak{p})$ and $S(\mathfrak{h}_\mathfrak{p})$ which are invariant under K and W respectively.

LEMMA 7 (Chevalley[14]). *For any $p \in I(\mathfrak{p})$ let $\bar{p}$ denote the restriction of the polynomial function p on $\mathfrak{h}_\mathfrak{p}$. Then $\bar{p} \in I(\mathfrak{h}_\mathfrak{p})$ and $p \to \bar{p}$ is an isomorphism of $I(\mathfrak{p})$ onto $I(\mathfrak{h}_\mathfrak{p})$.*

Now fix an element H_0 in $\mathfrak{h}_\mathfrak{p}$ and define W' as in Lemma 6. Put $J = I(\mathfrak{h}_\mathfrak{p})$ and let J' denote the algebra of those elements in $S(\mathfrak{h}_\mathfrak{p})$ which are invariant under W'.

LEMMA 8. *Let[15] $r = [W : W']$. Then there exist r homogeneous elements $v_1 = 1, v_2, \cdots, v_r$ in J' such that $J' = \sum_{1 \leqq i \leqq r} J v_i$. Moreover $v_1, \cdots, v_r$ are linearly independent over the quotient field of J.*

Put $S = S(\mathfrak{h}_\mathfrak{p})$ and let $C(S)$, $C(J')$ and $C(J)$ denote the quotient fields of S, J' and J respectively. Then $C(S)/C(J)$ is normal and its Galois group is W (see Chevalley [3(b), p. 781]). By the same argument W' is the Galois group of $C(S)/C(J')$. Hence $[C(J') : C(J)] = [W : W'] = r$. Let S_d denote the space of homogeneous elements in S of degree d. Then it is obvious that $J = \sum_{d \geqq 0} J_d$ and $J' = \sum_{d \geqq 0} J_d'$ where $J_d = S_d \cap J$ and $J_d' = S_d \cap J'$. Put $J_+ = \sum_{d \geqq 1} J_d$, $J_+' = \sum_{d \geqq 1} J_d'$. We claim that $J' \cap (SJ_+) = J'J_+$. For if $u = \sum_{1 \leqq i \leqq m} p_i u_i \in J'$ $(p_i \in S, u_i \in J_+)$, it is obvious that

$$u = u^s = \sum_i p_i^s u_i \qquad (s \in W')$$

and therefore $u = \sum_i q_i u_i \in J'J_+$ where $q_i = w'^{-1} \sum_{s \in W'} p_i^s$ and w' is the order of W'. Hence

---

[15] $[W : W']$ stands for the index of W' in W.

$$S/SJ_+ \supset (J' + SJ_+)/SJ_+ \cong J'/J' \cap SJ_+ = J'/J'J_+.$$

Moreover Chevalley has shown [3(b), Theorem (B)] that $\dim S/SJ_+ = w$ (where w is the order of W) and the natural representation of W on S/SJ_+ is equivalent to the regular representation of W. Hence in the reduction of this representation with respect to W', the trivial representation of W' occurs exactly $r = [W: W']$ times. Let S' be the set of those elements $u \in S$ whose residue class mod SJ_+ is left fixed by W'. Then $\dim S'/SJ_+ = r$. Moreover $u - u^s \in SJ_+$ for any $u \in S'$ and $s \in W'$ and therefore $u \equiv w'^{-1} \sum_{s \in W'} u^s$ mod SJ_+. This shows that $S' = J' + SJ_+$ and hence $S'/SJ_+ \cong J'/J'J_+$. Therefore $\dim J'/J'J_+ = r$ and so we can select r homogeneous elements $v_1 = 1, v_2, \cdots, v_r$ in J' such that their residue classes mod $J'J_+$ form a base for $J'/J'J_+$ over C. Let $V = \sum_{1 \leqq i \leqq r} Cv_i$. We shall prove that $J' = JV$. It is clear that $J' = V + J_+J'$ and from this it follows by induction that $J' = JV + J_+{}^mJ'$ for any integer $m \geqq 1$. In particular $J_d{}' \subset JV + J_+{}^mJ'$ for any $d \geqq 0$. But then by choosing $m > d$, it is obvious that $J_d{}' \subset JV$ and therefore $J' = \sum_{d \geqq 0} J_d{}' \subset JV$. This proves that $J' = JV$. Moreover since $C(J')/C(J)$ is a finite algebraic extension, it is clear that $C(J') = C(J)J' = C(J)V$. Therefore since $[C(J') : C(J)] = r$, $v_1, \cdots, v_r$ must be linearly independent over $C(J)$.

The above proof depended only on the fact that W and W' are finite groups generated by reflexions. Hence if we replace (W, W') by $(W, 1)$ and $(W', 1)$ respectively, we get the following corollary.

COROLLARY. *There exist homogeneous elements $u_1 = 1, u_2, \cdots, u_w$ and $u_1{}' = 1, u_2{}', \cdots, u_{w'}{}'$ in S such that*

$$S = \sum_{1 \leqq i \leqq w} Ju_i, \qquad S = \sum_{1 \leqq j \leqq w'} J'u_j{}'.$$

Moreover $(u_1, \cdots, u_w)$ are linearly independent over $C(J)$ and $(u_1{}', \cdots, u_{w'}{}')$ over $C(J')$.

Let $\mathfrak{m}$ denote the centralizer of $\mathfrak{h}_\mathfrak{p}$ in $\mathfrak{g}$ and $p(H)$ the determinant of the linear transformation on $\mathfrak{g}/\mathfrak{m}$ defined by $\operatorname{ad} H$ $(H \in \mathfrak{h}_\mathfrak{p})$. Then $p \in S$ and it is obvious that $p^s = p$ $(s \in W)$. Moreover $p(H) = \pm \prod_{\alpha \in P_+} \alpha(H)^2$. Hence if $\beta \in \Sigma$ and $s \in W$, it follows that either $s\beta$ or $-s\beta$ lies in Σ. Put $\langle H, H' \rangle = B(H, H')$ $(H, H' \in \mathfrak{h}_\mathfrak{p})$ and identify $\mathfrak{h}_\mathfrak{p}$ with its dual by means of the bilinear form B. We shall say that two nonzero linear functions λ, μ on $\mathfrak{h}_\mathfrak{p}$ are equivalent, if they are linearly dependent. Then if α and β are equivalent elements in Σ, $\beta = c\alpha$ where c is a positive real number.[16]

---

[16] Actually it is known (see Cartan [2]) that $c = \frac{1}{2}$, 1 or 2.

Let $l = \dim \mathfrak{h}_{\mathfrak{p}}$. Then we can select (see [5(1), Lemma 1]) l linearly independent elements $\alpha_1, \cdots, \alpha_l \in \Sigma$ such that every α in Σ can be written in the form $\alpha = m_1\alpha_1 + \cdots + m_l\alpha_l$ where m_i are nonnegative integers. Let q be the number of distinct equivalence classes in Σ. Extend $(\alpha_1, \cdots, \alpha_l)$ to a maximal set $(\alpha_1, \cdots, \alpha_q)$ of inequivalent elements in Σ and put $\pi = \alpha_1\alpha_2 \cdots \alpha_q \in S$. Since $p^s = p$ $(s \in W)$, it is obvious that $\pi^s = \epsilon(s)\pi$ where $\epsilon(s)$ is a real number. But the mapping $s \to \epsilon(s)$ is obviously a homomorphism of the finite group W into the multiplicative group of nonzero real numbers and therefore $\epsilon(s) = \pm 1$. We shall see presently that $\epsilon(s_\alpha) = -1$ for $\alpha \in \Sigma$.

Put $s_i = s_{\alpha_i}$ $1 \leqq i \leqq l$.

LEMMA 9. *W is generated by $(s_1, \cdots, s_l)$. Moreover for any $\alpha \in \Sigma$, we can choose $s \in W$ and an index i $(1 \leqq i \leqq l)$ such that α is equivalent to $s\alpha_i$.*

Let W_1 be the subgroup of W generated by $(s_1, \cdots, s_l)$ and α a given element in Σ. Then $\alpha = m_1\alpha_1 + \cdots + m_l\alpha_l$ where $m_1, \cdots, m_l$ are nonnegative integers. Put $m(\alpha) = m_1 + \cdots + m_l$. We shall prove by induction on $m(\alpha)$ that $\alpha = cs\alpha_i$ for some $s \in W_1$, some i $(1 \leqq i \leqq l)$ and a suitable positive number c. This is obvious if $m(\alpha) = 1$. So now suppose that $m(\alpha) \geqq 2$ and α is not equivalent to any α_i $(1 \leqq i \leqq l)$. Since $\langle \alpha, \alpha \rangle$ is positive, $\langle \alpha, \alpha_j \rangle$ is positive for some j. Moreover since α is not equivalent to α_j, $m_i > 0$ for some $i \neq j$. But $s_j\alpha = \alpha - 2\{\langle \alpha, \alpha_j \rangle / \langle \alpha_j, \alpha_j \rangle\}\alpha_j$ and $-s_j\alpha$ cannot lie in Σ since $m_i > 0$. Hence $s_j\alpha \in \Sigma$ and $m(\alpha) > m(s_j\alpha)$. Our assertion now follows by applying the induction hypothesis to $s_j\alpha$. Now if $\alpha = cs\alpha_i$, it is clear that $s_\alpha = ss_is^{-1} \in W_1$. Since s_α $(\alpha \in \Sigma)$ generate W, this proves that $W_1 = W$.

LEMMA 10. *$\epsilon(s_\alpha) = -1$ for $\alpha \in \Sigma$.*

We first claim that $\pi^{s_i} = -\pi$ $(1 \leqq i \leqq l)$. It is sufficient to prove this for $i = 1$. Obviously $s_1\alpha_1, s_1\alpha_2, \cdots, s_1\alpha_q$ are all inequivalent and therefore $s_1\alpha_j = c_j\alpha_j'$ $(1 \leqq j \leqq q)$ where $\alpha_j \to \alpha_j'$ is a permutation of the set $(\alpha_1, \alpha_2, \cdots, \alpha_q)$ and c_j are nonzero real numbers. Now suppose $j \neq 1$. Then if $\alpha_j = m_1\alpha_1 + \cdots + m_l\alpha_l$, $m_k > 0$ for some $k \neq 1$. On the other hand $s_1\alpha_j = \alpha_j + m\alpha_1$ for some integer m. Hence $-s_1\alpha_j$ cannot lie in Σ. Therefore $s_1\alpha_j \in \Sigma$ and $c_j > 0$. However $s_1\alpha_1 = -\alpha_1$ and so this proves that $\epsilon(s_1) = \prod_{1 \leqq j \leqq q} c_j < 0$. Hence $\epsilon(s_1) = -1$. Now let $\alpha \in \Sigma$. Then, as we have seen during the proof of Lemma 9, $s_\alpha = ss_is^{-1}$ for some $s \in W$ and some i $(1 \leqq i \leqq l)$. Therefore $\epsilon(s_\alpha) = \epsilon(s_i) = -1$.

We shall call an element $u \in S$ skew (or skew-invariant) if $u^s = \epsilon(s)u$ for $s \in W$.

COROLLARY. *$J\pi$ is exactly the set of all skew-invariants in S.*

Let S' be the set of all skew elements in S. It is obvious that $J\pi \subset S'$. Now suppose $u \in S'$. Then $u^{s_\alpha} = -u$ $(\alpha \in \Sigma)$ and therefore the polynomial function u vanishes identically on the hyperplane $\alpha = 0$ in $\mathfrak{h}_{\mathfrak{p}}$. But this implies that α divides u in S. This being true for every $\alpha \in \Sigma$, we conclude that $u = \pi v$ for some $v \in S$. But since both u and π are skew, it is clear that $v \in J$ and therefore $u \in J\pi$.

For any $x \in C(S)$, let $\mathrm{sp}_{S/J}x$ denote the relative trace of x from $C(S)$ to $C(J)$. Let $\mathfrak{D}_{S/J}$ be the set of those elements $x \in C(S)$ which have the property that $\mathrm{sp}_{S/J}xy \in J$ for every y in S.

LEMMA 11. *Let x be an element in $C(S)$. Then $x\mathfrak{D}_{S/J} \subset S$ if and only if $x \in S\pi$.*

Let y be any element in S. Since W is the Galois group of $C(S)/C(J)$, it is clear that $\mathrm{sp}_{S/J}(y/\pi) = \sum_{s \in W} (y/\pi)^s = y_0/\pi$ where $y_0 = \sum_{s \in W} \epsilon(s)y^s$. But y_0 is obviously a skew-invariant and therefore, from the corollary to Lemma 10, it lies in $J\pi$. This proves that $\pi^{-1} \in \mathfrak{D}_{S/J}$. Hence if x is an element in $C(S)$ such that $x\mathfrak{D}_{S/J} \subset S$, it follows that $x\pi^{-1} \in S$ and therefore $x \in S\pi$. The proof of the converse is however more complicated.

Select $u_i \in S$ $1 \leqq i \leqq w$ as in the corollary to Lemma 8 and let u^i $1 \leqq i \leqq w$ denote the dual base of $C(S)/C(J)$ so that[9] $\mathrm{sp}_{S/J}(u_i u^j) = \delta_i^j$ $(1 \leqq i, j \leqq w)$. Then it is easy to verify that $\mathfrak{D}_{S/J} = \sum_{1 \leqq i \leqq w} Ju^i$. Hence in order to complete the proof of our lemma, it is sufficient to show that $\pi u^i \in S$ $(1 \leqq i \leqq w)$. Fix an element α in Σ. In view of Lemma 9, we may assume that α is equivalent to $s\alpha_1$ for some $s \in W$. Let $\beta_1, \cdots, \beta_k$ be all the elements among $(\alpha_1, \cdots, \alpha_q)$ which are equivalent to $t\alpha$ for some $t \in W$. Put $\pi_\alpha = \beta_1\beta_2 \cdots \beta_k$. Then it is clear that $\pi_\alpha^s = c(s)\pi_\alpha$ where $c(s) = \pm 1$ $(s \in W)$. By the argument used in the proof of Lemma 10, we deduce easily that $c(s_1) = -1$ and therefore $c(s_\beta) = -1$ for $\beta = \beta_1, \beta_2, \cdots, \beta_k$. Now suppose $z \in J \cap S\alpha$. Then $z = y\alpha$ for some $y \in S$ and $z = z^{s_\alpha} = (y\alpha)^{s_\alpha} = -y^{s_\alpha}\alpha$. This shows that $y^{s_\alpha} = -y$ and therefore α divides y in S. But then α^2 divides z (in S). However $z \in J$ and therefore $(s\alpha)^2$ divides z for every $s \in W$. This shows that $z \in S\pi_\alpha^2$. Therefore since $\pi_\alpha^2 \in J$, we conclude, from the definition of J, that $z\pi_\alpha^{-2} \in S \cap C(J) = J$. This proves that $J \cap S\alpha = J\pi_\alpha^2$.

Let S_1 denote the set of all elements in $C(S)$ of the form a/b $(a, b \in S)$ where b and π_α are relatively prime in S. It is obvious that b^s and π_α are also relatively prime for every $s \in W$. Hence if $b_0 = \prod_{s \in W} b^s$ and $b_1 = b_0/b$, it follows that $a/b = ab_1/b_0$. Notice that b_0 lies in J but not in $J\pi_\alpha^2$. Moreover $S\alpha$ is obviously a prime ideal in S and therefore $J \cap S\alpha = J\pi_\alpha^2$ is a prime ideal in J. Hence if J_1 denotes the quotient ring of J with respect to $J\pi_\alpha^2$, b_0^{-1} lies in J_1 and this proves that $S_1 = SJ_1$. Finally if a/b is in $C(J)$, it is obvious that $ab_1 \in J$. Therefore $S_1 \cap C(J) = J_1$.

By a result of Chevalley [3(b), Theorem (A)], we can select $\omega_1, \cdots, \omega_l \in J$ such that $J = C[\omega_1, \cdots, \omega_l]$. Then $\omega_1, \cdots, \omega_l$ are algebraically independent (over C). Obviously π_α^2 is also transcendental over C and therefore we may assume that $(\pi_\alpha^2, \omega_2, \cdots, \omega_l)$ are algebraically independent so that $C(J)$ is algebraic over $C(\pi_\alpha^2, \omega_2, \cdots, \omega_l)$. Moreover since $\pi_\alpha^2 \in J$, it can be expressed as a polynomial in $\omega_1, \omega_2, \cdots, \omega_l$ with coefficient in C. ω_1 must actually appear in this polynomial because otherwise $\pi_\alpha^2, \omega_2, \cdots, \omega_l$ would be algebraically dependent. Therefore π_α^2 cannot divide (in J) any nonzero element in $C[\omega_2, \cdots, \omega_l]$. Hence the field $C_1 = C(\omega_2, \cdots, \omega_l)$ is contained in the local ring J_1.

Now we regard $C(J)/C_1$ and $C(S)/C_1$ as fields of algebraic functions of one variable (see Chevalley [3(a)]). It is obvious that π_α^2 is a prime element of J and therefore J_1 is a valuation ring in $C(J)$. Let p be the corresponding place of $C(J)/C_1$. For any j $(1 \leqq j \leqq k)$ and $x \in S$, let $\nu_j(x)$ denote the highest integer $m \geqq 0$ such that β_j^m divides x in S. (If $x = 0$ we put $\nu_j(x) = \infty$.) Then it is seen without difficulty that ν_j can be extended (uniquely) to a valuation of $C(S)$. Obviously J_1 is contained in the valuation ring of ν_j and therefore ν_j defines a place q_j of $C(S)$ lying above p. Since $C(S)$ is normal over $C(J)$, every place of $C(S)$ lying above p is conjugate to q_1 under W (see (see [3(a), p. 54]). But since $s\beta_1$ $(s \in W)$ is equivalent to β_j for some j, it follows that $q_1, q_2, \cdots, q_k$ are all the distinct places of $C(S)$ above p. It is obvious that S_1 is exactly the set of those elements in $C(S)$ which are integral at q_j for every j $(1 \leqq j \leqq k)$. Moreover $S_1 = J_1 S = \sum_{1 \leqq i \leqq w} J_1 u_i$. Since $\nu_j(\pi_\alpha^2) = 2$, it follows that the ramification index of q_j with respect to $C(J)$ is 2. Therefore we conclude from Theorem 7 of [3(a), p. 69] that the differential exponent of q_j is 1. Let $\mathfrak{D}_p$ be the set of all $x \in C(S)$ such that $\mathrm{sp}_{S/J} xS_1 \subset J_1$. Then obviously $\mathfrak{D}_p = \sum_{1 \leqq i \leqq w} J_1 u^i$. Hence it follows from Lemma 4 of [3(a), p. 73] that $\min_{1 \leqq i \leqq w} \nu_j(u^i) = -1$. Let d be a nonzero element in S of the lowest possible degree such that

$du^i \in S$ $1 \leqq i \leqq w$. Then the above result shows that π_α divides d in S and π_α and d/π_α are relatively prime in S. But since α was an arbitrary element in Σ, this implies that $d' = d/\pi$ lies in S and it is relatively prime to π. In order to complete our proof, it only remains to show that $d' \in C$.

We shall now introduce some notation which will also be useful later. For any $H \in \mathfrak{h}_\mathfrak{p}$, let S_H denote the set of all polynomial functions in S which vanish at H and put $J_H = J \cap S_H$. Obviously S_H and J_H are prime ideals in S and J respectively and $J_{sH} = J_H$ $(s \in W)$. Now suppose $\pi(H) \neq 0$. Then from Lemma 6, the w elements sH $(s \in W)$ are all distinct. Hence there exist w distinct prime ideals S_{sH} in S lying above J_H. On the other hand $J = C + J_H$ and therefore $S = \sum_{1 \leqq i \leqq w} Ju_i = \sum_{1 \leqq i \leqq w} Cu_i + SJ_H$. This proves that $\dim S/SJ_H \leqq w$. But in view of what we have said above, the associative algebra $\bar{S} = S/SJ_H$ has w distinct non-trivial homomorphisms into C. Therefore it must be semisimple and of dimension w and $\bigcap_{s \in W} S_{sH} = SJ_H$. Let $u \rightarrow \bar{u}$ denote the natural homomorphism of S on $\bar{S}$ and let $\mathrm{sp}\,\bar{u}$ denote the trace of $\bar{u}$ in the regular representation of $\bar{S}$. Then clearly $\mathrm{sp}\,\bar{u} = \sum_{s \in W} u(sH)$ $(u \in S)$. Moreover since $\bar{S}$ is semisimple, we can conclude that $\bar{u} = 0$ if $\mathrm{sp}\,\bar{u}_i\bar{u} = 0$ $(1 \leqq i \leqq w)$.

Now put $g_{ij} = \mathrm{sp}_{S/J}(u_iu_j)$ $1 \leqq i, j \leqq w$ and $g = \det(g_{ij})_{1 \leqq i,j \leqq w}$. Then $g \neq 0$. Let $(g^{ij})_{1 \leqq i,j \leqq w}$ denote the inverse of the matrix $(g_{ij})_{1 \leqq i,j \leqq w}$. It is obvious that $u^i = \sum_j g^{ij}u_j$ and therefore d divides g in S. We claim $g(H) \neq 0$. For otherwise we could choose complex numbers $c_1, \cdots, c_w$, not all zero, such that $\sum_j g_{ij}(H)c_j = 0$ $(1 \leqq i \leqq w)$. Put $u = \sum_j c_ju_j$. Then $\sum_j g_{ij}c_j = \mathrm{sp}_{S/J}(u_iu) = \sum_{s \in W} (u_iu)^s$. Hence $\mathrm{sp}\,\bar{u}_i\bar{u} = \sum_{s \in W} u_i(sH)u(sH) = 0$. But, as we have seen above, this implies that $\bar{u} = 0$. On the other hand $\bar{u}_1, \cdots, \bar{u}_w$ span $\bar{S}$ and so they must be linearly independent over C. Therefore $\bar{u} = \sum_j c_j\bar{u}_j \neq 0$ and we get a contradiction. Hence $g(H) \neq 0$ whenever $\pi(H) \neq 0$ $(H \in \mathfrak{h}_\mathfrak{p})$. This means that every prime factor of g divides π. But we know that π divides d and d divides g. Therefore π, d and g have exactly the same prime factors and this implies $d' \in C$. The proof of Lemma 11 is now complete.

Define W' and J' as before. We recall that $\pi = \alpha_1\alpha_2 \cdots \alpha_q$. Let π' denote the product of those elements among $\alpha_1, \cdots, \alpha_q$ which vanish at H_0. Define $\mathrm{sp}_{S/J'}x$ $(x \in C(S))$ to be the relative trace from $C(S)$ to $C(J')$.

COROLLARY. *Select u_i and u'_j $(1 \leqq i \leqq w, 1 \leqq j \leqq w')$ as in the corollary to Lemma* 8 *and define u^i and u'^j in $C(S)$ by the relations* $\mathrm{sp}_{S/J}(u^iu_k) = \delta_k^i$

$(1 \leqq i, k \leqq w)$ *and* $\mathrm{sp}_{S/J}(u'^j u'_m) = \delta_m{}^j$ $(1 \leqq j, m \leqq w')$ *respectively. Then* πu^i *and* $\pi' u'^j$ *are in* S. *Moreover if* d *and* d' *are any two elements in* S *such that* du^i *and* $d'u'^j$ $(1 \leqq i \leqq w, 1 \leqq j \leqq w')$ *are all in* S, *then* π *divides* d *and* π' *divides* d' *in* S.

We have already seen this for u^i. The proof for u'^j is entirely similar.
Choose $v_1, \cdots, v_r$ as in Lemma 8 and let $\mathrm{sp}_{J'/J}x$ $(x \in C(J'))$ denote the relative trace of x from $C(J')$ to $C(J)$.

LEMMA 12. *Define* $v^i \in C(J')$ $1 \leqq i \leqq r$ *by the conditions* $\mathrm{sp}_{J'/J}(v^i v_j) = \delta_j{}^i$ $(1 \leqq i, j \leqq r)$. *Then an element* $x \in S$ *is divisible by* π/π' *in* S *if and only if* $xv^i \in S$ $1 \leqq i \leqq r$.

Let D be a nonzero element in S of the least possible degree such that $Dv^i \in S$. Then the highest common factor (h. c. f.) of $Dv^1, \cdots, Dv^r$ (in S) is 1. Define u'^j as above. Then

$$\mathrm{sp}_{S/J}(u'^i v^j u'_k v_m) = \mathrm{sp}_{J'/J}\mathrm{sp}_{S/J'}(u'^i u'_k v^j v_m) = \delta_k{}^i \mathrm{sp}_{J'/J}(v^j v_m) = \delta_k{}^i \delta_m{}^j$$

$(1 \leqq i, k \leqq w', 1 \leqq j, m \leqq r)$. Since $S = \sum_{1 \leqq k \leqq w'} \sum_{1 \leqq m \leqq r} J v_m u'_k$, it follows from the corollary to Lemma 11 that $\pi u'^i v^j \in S$. Since the h. c. f. of Dv^j $(1 \leqq j \leqq r)$ is 1, this implies that $D^{-1}\pi u'^i \in S$. Therefore we conclude from the same corollary that $\pi/D\pi'$ is in S. Conversely $\pi' u'^i D v^j \in S$ and therefore π divides $\pi' D$ again by the same corollary. Hence $\pi' D/\pi$ lies in C and the lemma follows.

Put $J_H{}' = J' \cap S_H$ for $H \in \mathfrak{h}_{\mathfrak{p}}$.

LEMMA 13. $\dim J'/J'J_H = [W : W']$, $\dim S/SJ_H = w$ *and* $\dim S/SJ_H{}' = w'$ *for every* $H \in \mathfrak{h}_{\mathfrak{p}}$.

We prove only the first statement since the proofs of the other two are parallel. Suppose $\sum_{1 \leqq i \leqq r} c_i v_i \in J'J_H$ $(c_i \in C)$. Then since $J'J_H = \sum_i J_H v_i$, it follows from the linear independence of $v_1, \cdots, v_r$ over $C(J)$ (see Lemma 7) that $c_i \in J_H$. But obviously this implies that $c_i = 0$ $1 \leqq l \leqq r$. Hence the residue classes of $v_1, \cdots, v_r \bmod J'J_H$ form a base for $J'/J'J_H$ and therefore $\dim J'/J'J_H = r = [W : W']$.

Put $\sigma^i = \pi u^i$ $1 \leqq i \leqq w$. We have seen above that $\sigma^i \in S$.

LEMMA 14. *For any* $H \in \mathfrak{h}_{\mathfrak{p}}$, *let* $e_H = \sum_{1 \leqq i \leqq w} \sigma^i(H) u_i$. *Then*

(1) $pe_H \equiv p(H) e_H \bmod SJ_H$ *for any* $p \in S$,

(2) $\sum_{s \in W} \epsilon(s) e_{sH} \equiv \pi(H) \bmod SJ_H$,

(3) $e_{sH}(tH) = \epsilon(s)\pi(sH)$ *or zero according as* $s = t$ *or not* $(s, t \in W)$.

We know that

$$\delta_j^i = \mathrm{sp}_{S/J}(u^i u_j) = \sum_{s \in W} (u^i u_j)^s = \pi^{-1} \sum_{s \in W} \epsilon(s)(\sigma^i u_j)^s.$$

Therefore $\sum_{s \in W} \epsilon(s)(\sigma^i u_j)^s = \pi \delta_j^i$ $(1 \leqq i, j \leqq w)$. Now suppose $s_1, s_2, \cdots, s_w$ are all the distinct elements of W and $\pi(H) \neq 0$. Then this result implies that

$$\sum_k \epsilon(s_k)\sigma^i(s_k H) u_j(s_k H) = \pi(H)\delta_j^i.$$

Therefore if we regard

$$A = \{\sigma^i(s_k H)\}_{1 \leqq i, k \leqq w} \text{ and } B = \{u_j(s_k H)/\pi(H)\}_{1 \leqq k, j \leqq w}$$

as $w \times w$ matrices, it is clear that they are reciprocals of each other and therefore BA is also the unit matrix. Hence[9]

$$\sum_j \epsilon(s_i)\sigma^j(s_i H) u_j(s_k H) = \pi(H)\delta_{ik}.$$

This proves that $e_{s_i H}(s_k H) = \delta_{ik}\epsilon(s_i)\pi(H)$ and therefore $e_H \in S_{sH}$ if $s \neq 1$. Since $\pi(H) \neq 0$, we know (see the last part of the proof of Lemma 11) that $SJ_H = \bigcap_{s \in W} S_{sH}$. Therefore $e_H S_H \subset SJ_H$ and hence $pe_H \equiv p(H) e_H \bmod SJ_H$ for $p \in S$. Moreover it follows from the relation obtained above that $\sum_{s \in W} \epsilon(s) e_{sH}(tH) = \pi(H)$ for $t \in W$. Therefore $\sum_{s \in W} \epsilon(s) e_H - \pi(H) \in \bigcap_{t \in W} S_{tH} = SJ_H$. Thus all the statements of the lemma have been proved under the assumption that $\pi(H) \neq 0$.

Now we come to the general case. Select $x_{ij}^k \in J$ such that $u_i u_j = \sum_k x_{ij}^k u_k$. Then $e_H u_j = \sum_i \sigma^i(H) u_i u_j = \sum_{i,j} \sigma^i(H) x_{ij}^k u_k \equiv \sum_{i,k} \sigma^i(H) x_{ij}^k(H) u_k \bmod SJ_H$. But we know from Lemma 13 that $u_1, \cdots, u_w$ are linearly independent $\bmod SJ_H$. Therefore it is clear that the first statement of the lemma holds if and only $z_j^k(H) = 0$ $(1 \leqq j, k \leqq w)$ where $z_j^k = \sum_i \sigma^i x_{ij}^k - \sigma^k u_j$. But then it follows from the above proof that $z_j^k(H) = 0$ whenever $\pi(H) \neq 0$. Therefore since z_j^k are polynomial functions on $\mathfrak{h}_\mathfrak{p}$, we conclude that they are all zero. In the same way the second statement of the lemma is seen to be equivalent to the relations $\sum_{s \in W} \epsilon(s)\sigma^i(sH) = \pi(H)\delta_1^i$ $(1 \leqq i \leqq w)$. Again since these equations hold when $\pi(H) \neq 0$, they hold in general. The proof of (3) is entirely similar.

COROLLARY 1. *If* $\pi(H) \neq 0$ *then* e_{sH} $(s \in W)$ *are linearly independent* $\bmod SJ_H$.

This is an immediate consequence of the third statement of the above lemma.

COROLLARY 2. *Let p be an element in S and let $H \in \mathfrak{h}_{\mathfrak{p}}$. Consider the linear transformation L in S/SJ_H corresponding to multiplication by p. Then* $\det(tI - L) = \prod_{s \in W} (t - p(sH))$ *where t is an indeterminate and I is the identity mapping of S/SJ_H.*

Select $q_{ji} \in J$ such that $pu_i = \sum_j u_j q_{ji}$ $(1 \leqq i \leqq w)$. Then it is obvious that $pu_i \equiv \sum_j q_{ji}(H) u_j \bmod SJ_H$. Put

$$Q(t) = \det(t\delta_{ij} - q_{ij})_{1 \leqq i, j \leqq w}.$$

Then $Q(t)$ is a polynomial in t with coefficients in J. Obviously it is sufficient to prove that $Q(t) = \prod_{s \in W} (t - p^s)$. Let q_m and p_m denote the coefficients of t^m in $Q(t)$ and $\prod_{s \in W} (t - p^s)$ respectively. Put $Q(t:H) = \sum_{m \geqq 0} q^m(H) t^m$. If $\pi(H) \neq 0$, e_{sH} $(s \in W)$ form a base for $S \bmod SJ_H$ by Corollary 1 above and therefore it follows from the first statement of Lemma 14 that

$$Q(t:H) = \det(tI - L) = \prod_{s \in W} (t - p(sH)).$$

This shows that $q_m(H) = p_m(H)$ for every m, if $\pi(H) \neq 0$. But since q_m and p_m are polynomial functions on $\mathfrak{h}_{\mathfrak{p}}$, this implies that $q_m = p_m$.

Now put $D = \pi/\pi'$, $\tau^i = Dv^i$ $1 \leqq i \leqq r$ and select elements $s_1, \cdots, s_r$ in W such that $W = \bigcup_{1 \leqq i \leqq r} W' s_i$. (We recall that $r = [W : W']$.)

LEMMA 15. *Put* $f_H = \sum_{1 \leqq i \leqq r} \tau^i(H) v_i$ *for* $H \in \mathfrak{h}_{\mathfrak{p}}$. *Then*

(1) $pf_H \equiv p(H) f_H \bmod SJ_H$ *for* $p \in J'$,

(2) $\sum_{1 \leqq i \leqq r} \epsilon(s_i) \pi'(s_i H) f_{s_i H} \equiv \pi(H) \bmod SJ_H$,

(3) $f_{s_i H}(s_j H) = \delta_{ij} D(s_i H)$ $(1 \leqq i, j \leqq r)$.

Finally, $f_{s_1 H}, \cdots, f_{s_r H}$ *are linearly independent* $\bmod SJ_H$ *if* $\pi(H) \neq 0$.

The proof is similar to that of Lemma 14. Put $t_k = s_k^{-1}$ $(1 \leqq k \leqq r)$. Since $C(J')$ is the subfield of $C(S)$ consisting exactly of those elements which are left fixed by W', we conclude from Galois theory that $t_1, \cdots, t_r$ define all the distinct isomorphisms of $C(J')/C(J)$ into $C(S)$. Therefore $\mathrm{sp}_{J'/J} v = \sum_{1 \leqq i \leqq r} v^{t_i}$ for $v \in C(J')$. This shows that

$$\delta_j^i = \mathrm{sp}_{J'/J}(v^i v_j) = \sum_{1 \leqq k \leqq r} (\tau^i v_j / D)^{t_k}.$$

Multiplying this equation by π, we get

$$\sum_{1\leqq k\leqq r} \epsilon(t_k)\,(\pi'\tau^i v_j)^{t_k} = \pi\delta_j{}^i \qquad (1\leqq i, j\leqq r).$$

But this implies that

$$\sum_k \epsilon(s_k)\pi'(s_kH)\tau^i(s_kH)v_j(s_kH) = \pi(H)\delta_j{}^i.$$

Now first assume that $\pi(H)\neq 0$. Then the $r\times r$ matrices

$$A = \{\epsilon(s_k)\pi'(s_kH)\tau^i(s_kH)\}_{1\leqq i,k\leqq r} \text{ and } B = \{v_j(s_kH)/\pi(H)\}_{1\leqq k,j\leqq r}$$

are reciprocals of each other and therefore BA is also the unit matrix. Hence

$$\sum_k \epsilon(s_i)\pi'(s_iH)\tau^k(s_iH)v_k(s_jH) = \pi(H)\delta_{ij}$$

and this proves that $f_{s_iH}(s_jH) = \delta_{ij}D(s_iH)$ $1\leqq i, j\leqq r$. (By continuity this relation remains valid even when $\pi(H)=0$.) Since $\pi(H)\neq 0$, it is clear that $D(sH)\neq 0$ for any $s\in W$. Therefore the linear independence of $f_{s_1H},\cdots,f_{s_rH} \bmod SJ_H$ is obvious. Furthermore

$$\sum_{1\leqq i\leqq r} \epsilon(s_i)\pi'(s_iH)f_{s_iH}(s_jH) = \epsilon(s_j)\pi'(s_jH)D(s_jH) = \pi(H) \qquad (1\leqq i\leqq r).$$

On the other hand $f_{s_iH}\in J'$ and therefore $f_{s_iH}(sH) = f_{s_iH}(s_jH)$ if $s\in W's_j$. Hence if we put $g = \sum_{1\leqq i\leqq r}\epsilon(s_i)\pi'(s_iH)f_{s_iH} - \pi(H)$, it follows that $g(sH)=0$ for all $s\in W$. But this implies that $g\in\bigcap_{s\in W} S_{sH} = SJ_H$ and so we get the second statement of the lemma. Now suppose $p\in J'$. Then $p(sH) = p(H)$ for $s\in W'$ and therefore $p - p(H)\in\bigcap_{s\in W'} S_{sH}$. On the other hand we have seen above that $f_H(sH) = 0$ if $s\notin W'$. Therefore $(p-p(H))f_H\in\bigcap_{s\in W} S_{sH}$ $= SJ_H$ and this proves that $pf_H\equiv p(H)f_H \bmod SJ_H$.

In order to extend our results to the general case, we use the same method as before. For example, let us prove the first statement. It is enough to show that $v_if_H\equiv v_i(H)f_H \bmod SJ_H$ $1\leqq i\leqq r$. Since $w'v = \sum_{s\in W'} v^s$ for $v\in J'\cap(SJ_H)$, it follows that $J'\cap(SJ_H) = J'J_H$. Select $y_{ij}{}^k\in J$ such that $v_iv_j = \sum_k y_{ij}{}^kv_k$. Then due to Lemma 13, the required relations hold if and only if $\sum_j \tau^j(H)y_{ij}{}^k(H) = v_i(H)\tau^k(H)$ $(1\leqq i, k\leqq r)$. The remaining argument is now the same as in the proof of Lemma 14.

COROLLARY. *Let p be an element in J' and let $H\in\mathfrak{h}_{\mathfrak{p}}$. Consider the linear transformation L' in $J'/J'J_H$ corresponding to multiplication by p.*

Then $\det(tI'-L')=\prod_{1\leqq i\leqq r}(t-p(s_iH))$ *where* t *is an indeterminate and* I' *is the identity mapping of* $J'/J'J_H$.

This is proved in the same way as Corollary 2 to Lemma 14.

Define J_+ as in the proof of Lemma 8 and let d_π and d_i denote the degrees of π and u_i $(1\leqq i\leqq w)$ respectively. Then the following result is of some interest, although it is not strictly necessary for our purpose. Therefore we state it here without proof.

LEMMA 16. *Suppose* $d_w=\max_{1\leqq i\leqq w} d_i$. *Then* $d_w=d_\pi$ *and* $d_i<d_\pi$ *for* $1\leqq i\leqq w$. *Moreover* $u_w\equiv c\pi \bmod SJ_+$ *where* c *is a nonzero complex number.*

4. The homomorphism γ. We now return to the notation of Section 2 and for any $q\in I_{\mathfrak{g}}$ define $u_q\in\mathfrak{H}_{\mathfrak{p}}$ as in Lemma 3. Put $\rho=\frac{1}{2}\sum_{\alpha\in P_+}\bar{\alpha}$ where $\bar{\alpha}$ denotes the restriction of α on $\mathfrak{h}_{\mathfrak{p}}$. Also let $u\rightarrow{}'u$ denote the automorphism of $\mathfrak{H}_{\mathfrak{p}}$ such that ${}'H=H-\rho(H)$ $(H\in\mathfrak{h}_{\mathfrak{p}})$. We identify $S(\mathfrak{h}_{\mathfrak{p}})$ with $\mathfrak{H}_{\mathfrak{p}}$ under the isomorphism which preserves every element of $\mathfrak{h}_{\mathfrak{p}}$. Then $J=I(\mathfrak{h}_{\mathfrak{p}})$ becomes a subalgebra of $\mathfrak{H}_{\mathfrak{p}}$. Put $\gamma(q)={}'u_q$ $(q\in I_{\mathfrak{g}})$.

THEOREM 1. γ *is a homomorphism of* $I_{\mathfrak{g}}$ *onto* $I(\mathfrak{h}_{\mathfrak{p}})$ *and its kernel is* $I_{\mathfrak{g}}\cap\mathfrak{B}\mathfrak{k}=I_{\mathfrak{g}}\cap\mathfrak{k}\mathfrak{B}$.

In order to show that γ is a homomorphism, it is enough to verify that $u_{q_1q_2}=u_{q_1}u_{q_2}$ for $q_1,q_2\in I_{\mathfrak{g}}$. Now $q_2-u_{q_2}\in\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{n}$. Therefore $q_1(q_2-u_{q_2})\in\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{n}$ since $q_1\mathfrak{k}=\mathfrak{k}q_1$. But $q_1u_{q_2}=(q_1-u_{q_1})u_{q_2}+u_{q_1}u_{q_2}$ and $(q_1-u_{q_1})u_{q_2}\in(\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{n})u_{q_2}\subset\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{n}$ since $[\mathfrak{n},\mathfrak{h}_{\mathfrak{p}}]\subset\mathfrak{n}$. Therefore $q_1q_2-u_{q_1}u_{q_2}\in\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{n}$ and this proves that $u_{q_1q_2}=u_{q_1}u_{q_2}$.

Now fix q in $I_{\mathfrak{g}}$. Then it follows from Lemma 4 that $\gamma(q)=0$ if and only if $\chi_\nu(u_q)=0$ for every $\nu\in\mathfrak{F}_0$. Define π and ϕ as in Lemma 5 and put $g(x)=(\phi,\pi(x)\phi)$ for $x\in G$. Then if ν denotes the restriction on $\mathfrak{h}_{\mathfrak{p}}$ of the highest weight of π, it follows from Lemma 3 that $g(x;q)=\chi_\nu(u_q)g(x)$. Since $g(1)=1$, this shows that $\chi_\nu(u_q)=g(1;q)$. But since g is spherical, it is clear that $g(1;q)=0$ if $q\in\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{k}$. Hence $I_{\mathfrak{g}}\cap(\mathfrak{k}\mathfrak{B}+\mathfrak{B}\mathfrak{k})$ is contained in the kernel of γ. On the other hand $\gamma(q)=0$ implies that $g(x;q)=(\phi,\pi(x)\pi(q)\phi)=0$. Since this holds for every x in G and since π is irreducible, it follows that $\pi(q)\phi=0$. Therefore by applying Lemma 1 of [5(d)] to $\mathfrak{Y}=\mathfrak{X}\mathfrak{k}$, we conclude that $q\in\mathfrak{B}\mathfrak{k}$. Combining this with the above result, we deduce that $I_{\mathfrak{g}}\cap\mathfrak{B}\mathfrak{k}$ is exactly the kernel of γ and therefore $I_{\mathfrak{g}}\cap\mathfrak{B}\mathfrak{k}\supset I_{\mathfrak{g}}\cap\mathfrak{k}\mathfrak{B}$. Now consider the anti-automorphism $b\rightarrow b^*$ of $\mathfrak{B}$ such that $X^*=-X$ for every $X\in\mathfrak{g}$. It is obvious that $I_{\mathfrak{g}}{}^*=I_{\mathfrak{g}}$. Hence

$(I_\mathfrak{g} \cap \mathfrak{B}\mathfrak{k})^* = I_\mathfrak{g} \cap \mathfrak{k}\mathfrak{B} \supset (I_\mathfrak{g} \cap \mathfrak{k}\mathfrak{B})^* = I_\mathfrak{g} \cap \mathfrak{B}\mathfrak{k}$. This proves that $I_\mathfrak{g} \cap \mathfrak{B}\mathfrak{k} = I_\mathfrak{g} \cap \mathfrak{k}\mathfrak{B}$.

In order to prove that γ maps $I_\mathfrak{g}$ into J we need some additional facts. For any $h \in A_\mathfrak{p}$ and $s \in W$, put $h^s = \exp(sH)$ where $H = \log h$ and let dn denote the Haar measure on N.

LEMMA 17. *Put*

$$F_f(h) = e^{\rho(\log h)} \int_N f(hn)\, dn \qquad (h \in A_\mathfrak{p})$$

for any function f in[17] *$C_c^\infty(G)$ such that $f(kxk^{-1}) = f(x)$ $(x \in G, k \in K)$. Then $F_f(h^s) = F_f(h)$ for $s \in W$ and $h \in A_\mathfrak{p}$.*

Let $x \to x^*$ denote the natural mapping of G on the factor space $G^* = G/A_\mathfrak{p}$. Put $D(h) = \prod_{\alpha \in P_+} (e^{\alpha(H)/2} - e^{-\alpha(H)/2})$ and $h^{x^*} = xhx^{-1}$ $(h \in A_\mathfrak{p}, x \in G)$ where $H = \log h$. Denote the invariant measure on G^* by dx^* and consider the set $A_\mathfrak{p}'$ of those elements $h \in A_\mathfrak{p}$ where $D(h) \neq 0$. Then[18] the integral $\int_{G^*} g(h^{x^*})\, dx^*$ is convergent for $g \in C_c(G)$ and $h \in A_\mathfrak{p}'$. Moreover the measure dn can be so normalized that

$$|D(h)| \int_{G^*} g(h^{x^*})\, dx^* = e^{\rho(\log h)} \int_{K \times N} g(khnk^{-1})\, dk\, dn \qquad (h \in A_\mathfrak{p}').$$

Let s be an element in W and select k in K such that $khk^{-1} = h^s$ for $h \in A_\mathfrak{p}$. Then for any $x \in G$, the coset $(xk)^*$ depends only on x^* and s and we denote it by x^*s. Since W is a finite group, it follows without difficulty that the measure dx^* is invariant under these operations of W on G^*. Therefore

$$\int_{G^*} g((h^s)^{x^*})\, dx^* = \int_{G^*} g(h^{x^*})\, dx^*$$

for $g \in C_c(G)$ and $h \in A_\mathfrak{p}'$. If we apply this to f and make use of the fact that $|D(h^s)| = |D(h)|$, it follows that $F_f(h^s) = F_f(h)$ for $h \in A_\mathfrak{p}'$. However it is obvious from its definition that $F_f \in C_c^\infty(A_\mathfrak{p})$. Therefore $F_f(h^s) = F_f(h)$ for all $h \in A_\mathfrak{p}$.

COROLLARY. *For any linear function λ on $\mathfrak{h}_\mathfrak{p}$, put*

$$\phi_\lambda(x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) - \rho(H(xk))\}\, dk \qquad (x \in G).$$

Then $\phi_{s\lambda} = \phi_\lambda$ for $s \in W$.

---

[17] See footnote 1 of [5(k)] for notation.

[18] The facts stated here are quite well known. In any case their proofs offer no difficulty (see [5(f), p. 508]).

Obviously ϕ_λ is a spherical function of class C^∞. Hence if dx is the Haar meaure on G, it would be enough to show that for a fixed s,

$$\int \phi_\lambda(x) f(x)\,dx = \int \phi_{s\lambda}(x) f(x)\,dx$$

for every spherical function f in $C_c^\infty(G)$. Let dh denote the Haar measure on $A_{\mathfrak{p}}$. Then it is possible (see [5(c), Lemma 35]) to normalize it in such a way that $dx = e^{2\rho(\log h)} dk dh dn$ if $x = khn$ $(k \in K, h \in A_{\mathfrak{p}}, n \in N)$. Therefore

$$\begin{aligned}\int \phi_\lambda(x) f(x)\,dx &= \int \exp\{(-1)^{\frac{1}{2}}\lambda(H(x)) - \rho(H(x))\} f(x)\,dx \\ &= \int \exp\{(-1)^{\frac{1}{2}}\lambda(\log h) + \rho(\log h)\} f(hn)\,dh dn \\ &= \int \exp\{(-1)^{\frac{1}{2}}\lambda(\log h)\} F_f(h)\,dh.\end{aligned}$$

Our assertion now follows immediately from the above lemma.

Now suppose $q \in I_{\mathfrak{g}}$. Then $\gamma(q)$, being an element of $S(\mathfrak{h}_{\mathfrak{p}})$, can be regarded as a polynomial function on $\mathfrak{h}_{\mathfrak{p}}$. We denote by $\gamma(q:H)$ the value of this function at $H \in \mathfrak{h}_{\mathfrak{p}}$. Also let us recall that $\mathfrak{h}_{\mathfrak{p}}$ has been identified with its dual under the bilinear form B. Hence the following result is an immediate consequence of Lemma 3 and the definition of $\gamma(q)$.

LEMMA 18. *$\phi_\lambda(x;q) = \gamma(q:(-1)^{\frac{1}{2}}\lambda)\phi_\lambda(x)$ for $q \in I_{\mathfrak{g}}$, $x \in G$ and any linear function λ on $\mathfrak{h}_{\mathfrak{p}}$.*

It is obvious from this lemma and the corollary to Lemma 17 that $\gamma(q:H) = \gamma(q:sH)$ for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}}$. Hence $\gamma(q) = \gamma(q)^s$ and this proves that $\gamma(q) \in J$.

We still have to show that γ maps $I_{\mathfrak{g}}$ *onto* J. Le λ denote the canonical mapping (see [5(c), p. 192]) of[11] $S(\mathfrak{g})$ onto $\mathfrak{B}$ and put $\mathfrak{P} = \lambda(S(\mathfrak{p}))$ and $\mathfrak{P}_d = \lambda(S_d(\mathfrak{p}))$ where $S_d(\mathfrak{p})$ is the set of all homogeneous elements in $S(\mathfrak{p})$ of degree d. Since $\mathfrak{g}$ is the direct sum of $\mathfrak{k}$ and $\mathfrak{p}$, it follows [5(c), Lemma 12] that $\mathfrak{B} = \mathfrak{K}\mathfrak{P}$ and therefore $\mathfrak{B} = \mathfrak{P} + \mathfrak{k}\mathfrak{B}$, the sum being direct. Moreover if $X \in \mathfrak{k}$ it is obvious that both $\mathfrak{P}$ and $\mathfrak{k}\mathfrak{B}$ are invariant under the mapping[19] $b \rightarrow [X, b]$ $(b \in \mathfrak{B})$ of $\mathfrak{B}$. Hence $I_{\mathfrak{g}} = I_{\mathfrak{g}} \cap \mathfrak{P} + I_{\mathfrak{g}} \cap \mathfrak{k}\mathfrak{B}$ and so it is sufficient to prove the following lemma.

LEMMA 19. *γ defines a linear isomorphism of $I_{\mathfrak{g}} \cap \mathfrak{P}$ onto J.*

Since $I_{\mathfrak{g}} \cap \mathfrak{k}\mathfrak{B}$ is the kernel of γ and $\mathfrak{P} \cap \mathfrak{k}\mathfrak{B} = \{0\}$, it is clear that γ is univalent on $I_{\mathfrak{g}} \cap \mathfrak{P}$. Also it follows from Lemma 11 of [5(c)] that

---

[19] $[a, b] = ab - ba$ for $a, b \in \mathfrak{B}$.

$I_{\mathfrak{g}} \cap \mathfrak{P} = \lambda(I(\mathfrak{p}))$ (in the notation of Lemma 7). Let u be a homogeneous element in J of degree d. We shall prove by induction on d that there exists an element $q \in \sum_{e \leqq d} I_{\mathfrak{g}} \cap \mathfrak{P}_e$ such that $\gamma(q) = u$. This is obvious if $d = 0$. So suppose $d \geqq 1$. Let $\bar{p}$ denote the restriction on $\mathfrak{h}_{\mathfrak{p}}$ of any polynomial function $p \in S(\mathfrak{g})$. By Lemma 7, we can select a homogeneous element $p_0 \in I(\mathfrak{p})$ of degree d such that $\bar{p}_0 = u$. Put $q_0 = \lambda(p_0)$. Then q_0 lies in $I_{\mathfrak{g}} \cap \mathfrak{P}$. We shall prove that $u - \gamma(q_0)$ is of degree lower than d and hence, by induction hypothesis, we can choose $q_1 \in I_{\mathfrak{g}} \cap \mathfrak{P}$ of degree $< d$ such that $u - \gamma(q_0) = \gamma(q_1)$. Then $u = \gamma(q)$ where $q = q_0 + q_1$ and this would prove the lemma.

We know that $\mathfrak{g}$ is the direct sum of $\mathfrak{k}$, $\mathfrak{h}_{\mathfrak{p}}$ and $\mathfrak{n}$. Hence[11] $S(\mathfrak{g}) = S(\mathfrak{k})S(\mathfrak{h}_{\mathfrak{p}})S(\mathfrak{n})$. Now $\mathfrak{h}_{\mathfrak{p}}$ is orthogonal to $\mathfrak{k} + \mathfrak{n}$ under the bilinear form $B(X,Y)$ $(X, Y \in \mathfrak{g})$. Hence if $p \in \mathrm{S}(\mathfrak{g})$, it is obvious that $p - \bar{p} \in \mathfrak{k}S(\mathfrak{g}) + \mathrm{S}(\mathfrak{g})\mathfrak{n}$ (the products being taken in $S(\mathfrak{g})$). Therefore it is clear that $p_0 - u \in \mathfrak{k}S_{d-1}(\mathfrak{g}) + S_{d-1}(\mathfrak{g})\mathfrak{n}$, where $S_e(\mathfrak{g})$ denotes the space of homogeneous elements in $S(\mathfrak{g})$ of degree e. But then

$$q_0 - u \in \lambda(\mathfrak{k}S_{d-1}(\mathfrak{g}) + S_{d-1}(\mathfrak{g})\mathfrak{n}).$$

On the other hand if $f_1 \in S_{e_1}(\mathfrak{g})$, $f_2 \in S_{e_2}(\mathfrak{g})$, we know (see [5(a), p. 902]) that

$$\lambda(f_1 f_2) - \lambda(f_1)\lambda(f_2) \in \sum_{e < e_1 + e_2} \lambda(S_e(\mathfrak{g})).$$

Therefore

$$q_0 - u \in \mathfrak{k}\mathfrak{B} + \mathfrak{B}\mathfrak{n} + \sum_{e<d} \lambda(S_e(\mathfrak{g})).$$

Hence it follows from Lemma 3 and the definition of γ that $\gamma(q_0) - u$ is of degree $< d$. The proof of Theorem 1 is now complete.[20]

The following result, which we note here for later use, has been obtained during the above proof.

LEMMA 20. *Let λ denote the canonical mapping of $S(\mathfrak{g})$ onto $\mathfrak{B}$. Then if p is any homogeneous element of degree d in $I(\mathfrak{p})$, $\gamma(\lambda(p)) - \bar{p}$ is of degree $< d$. (Here $\bar{p}$ denotes the restriction of p on $\mathfrak{h}_{\mathfrak{p}}$.)*

5. The mapping $\mathfrak{S}'$.

Put $\Delta(H) = \prod_{\alpha \in P_+} (e^{\alpha(H)} - e^{-\alpha(H)})$ $(H \in \mathfrak{h}_{\mathfrak{p}})$ and $\Delta(h) = \Delta(\log h)$ $(h \in A_{\mathfrak{p}})$. We call a point h in $A_{\mathfrak{p}}$ singular or regular according as $\Delta(h) = 0$ or not. Let $A_{\mathfrak{p}}'$ denote the set of regular points in $A_{\mathfrak{p}}$. We regard $\mathfrak{g}$ as a Hilbert space under the positive-definite Hermitian form

---

[20] Although our definition of γ makes use of an order in the space of real linear functions on $\mathfrak{h}_{\mathfrak{p}_0}$, it can be shown that γ is actually independent of the choice of this order (cf. [5(g), Lemma 20]).

$-B(X, \tilde{\theta}(X))$ $(X \in \mathfrak{g})$ where $\tilde{\theta}$ denotes the conjugation of $\mathfrak{g}$ with respect to its compact real form $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$. Let $\mathfrak{m}$ be the centralizer of $\mathfrak{h}_\mathfrak{p}$ in $\mathfrak{g}$ and $\mathfrak{q}$ the orthogonal complement of $\mathfrak{m}$ in $\mathfrak{g}$. Then $\mathfrak{m} \cap \mathfrak{p} = \mathfrak{h}_\mathfrak{p}$ (because $\mathfrak{h}_\mathfrak{p}$ is maximal abelian in $\mathfrak{p}$) and $\mathfrak{q} = \mathfrak{q}_\mathfrak{k} + \mathfrak{q}_\mathfrak{p}$ where $\mathfrak{q}_\mathfrak{k} = \mathfrak{q} \cap \mathfrak{k}$ and $\mathfrak{q}_\mathfrak{p} = \mathfrak{q} \cap \mathfrak{p}$.

Lemma 21. *Suppose $h \in A_\mathfrak{p}'$. Then $\mathfrak{g} = \mathrm{Ad}(h^{-1})\mathfrak{q}_\mathfrak{k} + \mathfrak{h}_\mathfrak{p} + \mathfrak{k}$ where the sum is direct.*

It is known [5(c), Lemma 4] that $\dim \mathfrak{q}_\mathfrak{k} = \dim \mathfrak{q}_\mathfrak{p}$. On the other hand $\dim \mathfrak{g} = \dim \mathfrak{k} + \dim \mathfrak{p}$ and $\mathfrak{p}$ is the orthogonal sum of $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{q}_\mathfrak{p}$. Hence $\dim \mathfrak{g} = \dim \mathfrak{k} + \dim \mathfrak{h}_\mathfrak{p} + \dim \mathfrak{q}_\mathfrak{p} = \dim \mathfrak{k} + \dim \mathfrak{h}_\mathfrak{p} + \dim \mathfrak{q}_\mathfrak{k}$. Therefore it is sufficient to prove that $\mathrm{Ad}(h^{-1})\mathfrak{q}_\mathfrak{k} \cap (\mathfrak{h}_\mathfrak{p} + \mathfrak{k}) = \{0\}$. Let X be an element of $\mathfrak{q}_\mathfrak{k}$ such that $\mathrm{Ad}(h^{-1})X \in \mathfrak{h}_\mathfrak{p} + \mathfrak{k}$ and put $Y = (\mathrm{ad}\, H)^2 X$ where H is some element in $\mathfrak{h}_{\mathfrak{p}_0}$. Then $Y \in \mathfrak{k}$ and $\mathrm{Ad}(h^{-1})Y \in \mathfrak{k}$. Therefore $\mathrm{Ad}(h)Y = \theta(\mathrm{Ad}(h^{-1})Y) = \mathrm{Ad}(h^{-1})Y$ where θ is defined as usual (see [5(c), p. 187]). But since $h \in A_\mathfrak{p}'$, $\mathfrak{m}$ is the centralizer of h^2 in $\mathfrak{g}$ and therefore $Y \in \mathfrak{m}$. This means that $(\mathrm{ad}\, H)^3 X = (\mathrm{ad}\, H) Y = 0$. However $\mathrm{ad}\, H$ is a self-adjoint operator on $\mathfrak{g}$ and so we conclude that $[H, X] = 0$. This being true for every $H \in \mathfrak{h}_{\mathfrak{p}_0}$, it follows that $X \in \mathfrak{m}$. But $\mathfrak{m} \cap \mathfrak{q} = \{0\}$, and therefore $X = 0$. This proves the lemma.

Let $\mathfrak{Q}_\mathfrak{k}$ be the image of[11] $S(\mathfrak{q}_\mathfrak{k})$ in $\mathfrak{B}$ under the canonical mapping.

Corollary 1. *The mapping*[12] $q \times v \times x \rightarrow q^{h^{-1}} v x$ $(q \in \mathfrak{Q}_\mathfrak{k}, v \in \mathfrak{H}_\mathfrak{p}, x \in \mathfrak{X})$ *defines a linear isomorphism of the tensor product $\mathfrak{Q}_\mathfrak{k} \times \mathfrak{H}_\mathfrak{p} \times \mathfrak{X}$ onto $\mathfrak{B}$ if $h \in A_\mathfrak{p}'$.*

This is an immediate consequence of the above result and Lemma 12 of [5(c)].

Put $\mathfrak{m}_\mathfrak{k} = \mathfrak{m} \cap \mathfrak{k}$ and let $\mathfrak{M}_\mathfrak{k}$ be the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{m}_\mathfrak{k})$. Since $\mathfrak{k} = \mathfrak{m}_\mathfrak{k} + \mathfrak{q}_\mathfrak{k}$, it follows from Lemma 12 of [5(c)] that $\mathfrak{X} = \mathfrak{Q}_\mathfrak{k}\mathfrak{M}_\mathfrak{k}$. Let $\mathfrak{Q}_\mathfrak{k}'$ denote the set of those elements in $\mathfrak{Q}_\mathfrak{k}$ whose homogeneous component[21] of degree zero is zero. Since $[\mathfrak{m}_\mathfrak{k}, \mathfrak{q}_\mathfrak{k}] \subset \mathfrak{q}_\mathfrak{k}$, it follows without difficulty that

$$\mathfrak{X}\mathfrak{k} = \mathfrak{k}\mathfrak{X} = \mathfrak{Q}_\mathfrak{k}'\mathfrak{M}_\mathfrak{k} + \mathfrak{Q}_\mathfrak{k}\mathfrak{M}_\mathfrak{k}\mathfrak{m}_\mathfrak{k}.$$

Hence in particular $\mathfrak{k}\mathfrak{Q}_\mathfrak{k} \subset \mathfrak{Q}_\mathfrak{k}'\mathfrak{M}_\mathfrak{k} + \mathfrak{Q}_\mathfrak{k}\mathfrak{M}_\mathfrak{k}\mathfrak{m}_\mathfrak{k}$. Moreover $\mathfrak{B} = (\mathfrak{Q}_\mathfrak{k})^{h^{-1}}\mathfrak{H}_\mathfrak{p}\mathfrak{X}$. from the above corollary and therefore $(\mathrm{Ad}(h^{-1})\mathfrak{k})\mathfrak{B} = (\mathfrak{k}\mathfrak{Q}_\mathfrak{k})^{h^{-1}}\mathfrak{H}_\mathfrak{p}\mathfrak{X}$. Since $[\mathfrak{m}, \mathfrak{h}_\mathfrak{p}] = \{0\}$, this implies that

---

[21] Define λ and $S_d(\mathfrak{g})$ as during the proof of Lemma 19. Then $\mathfrak{B}$ is the direct sum of $\lambda(S_d(\mathfrak{g}))$ $(d \geqq 0)$ and an element $b \in \mathfrak{B}$ is homogeneous of degree d if $b \in \lambda(S_d(\mathfrak{g}))$.

$$\mathfrak{k}^{h^{-1}}\mathfrak{B} \subset (\mathfrak{Q}_{\mathfrak{k}}')^{h^{-1}}\mathfrak{H}_{\mathfrak{p}}\mathfrak{X} + \mathfrak{B}\mathfrak{k}$$

and therefore

$$\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k} = (\mathfrak{Q}_{\mathfrak{k}}')^{h^{-1}}\mathfrak{H}_{\mathfrak{p}}\mathfrak{X} + (\mathfrak{Q}_{\mathfrak{k}})^{h^{-1}}\mathfrak{H}_{\mathfrak{p}}\mathfrak{X}\mathfrak{k}.$$

Combining this with Corollary 1 above, we get the following result.

COROLLARY 2. *$\mathfrak{B}$ is the direct sum of $\mathfrak{H}_{\mathfrak{p}}$ and $\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k}$ if $h \in A_{\mathfrak{p}}'$.*

But this obviously implies the lemma below.

LEMMA 22. *Let h be an element in $A_{\mathfrak{p}}'$. Then for any $b \in \mathfrak{B}$ there exists a unique element $\delta_h'(b) \in \mathfrak{H}_{\mathfrak{p}}$ such that*

$$b - \delta_h'(b) \in \mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k}.$$

The significance of $\delta_h'(b)$ is given by the following lemma.[22]

LEMMA 23. *Let ϕ be a spherical function on G of class C^{∞}. Then*[11]

$$\phi(h;b) = \phi(h;\delta_h'(b))$$

for $b \in \mathfrak{B}$ and $h \in A_{\mathfrak{p}}'$.

Since ϕ is spherical, it is obvious that $\phi(h;b') = 0$ for $b' \in \mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k}$. Therefore our assertion follows from the definition of $\delta_h'(b)$.

Now we regard $A_{\mathfrak{p}}'$ as an open submanifold (see [5(g), p. 110]) of the Lie group $A_{\mathfrak{p}}$. Then if $b \in \mathfrak{B}$, we intend to show that there exists a differential operator $\delta'(b)$ on $A_{\mathfrak{p}}'$ whose local expression (see [5(g), p. 112]) at any point $h \in A_{\mathfrak{p}}'$ coincides with $\delta_h'(b)$.

Define π as in Lemma 11 and let $\mathfrak{h}_{\mathfrak{p}_0}'$ be the set of those points $H \in \mathfrak{h}_{\mathfrak{p}_0}$ where $\pi(H) \neq 0$. It is obvious that $\mathfrak{h}_{\mathfrak{p}_0}'$ is mapped onto $A_{\mathfrak{p}}'$ under the exponential mapping. Let $\mathfrak{R}$ be the ring of analytic functions on $A_{\mathfrak{p}}'$ generated[23] (over C) by the functions g_{β} ($\beta \in P_{+}$) defined by

$$g_{\beta}(\exp H) = (e^{2\beta(H)} - 1)^{-1} \qquad (H \in \mathfrak{h}_{\mathfrak{p}_0}').$$

Note that $Hg_{\beta} = -2\beta(H)(g_{\beta} + g_{\beta}^{2})$ for $H \in \mathfrak{h}_{\mathfrak{p}}$ and therefore $\mathfrak{R}$ is stable under the action of any differential operator in $\mathfrak{H}_{\mathfrak{p}}$. Let $\mathfrak{B}_d$ denote the space of all elements in $\mathfrak{B}$ of degree $\leqq d$.

LEMMA 24. *Let b be an element in $\mathfrak{B}_d$. Then we can choose $u \in \mathfrak{H}_{\mathfrak{p}} \cap \mathfrak{B}_d$ and a finite set of elements $v_i \in \mathfrak{H}_{\mathfrak{p}} \cap \mathfrak{B}_{d-1}$ and $g_i \in \mathfrak{R}$ $(1 \leqq i \leqq r)$ such that*

---

[22] On account of our identification of $\mathfrak{H}_{\mathfrak{p}}$ with $S(\mathfrak{h}_{\mathfrak{p}})$, elements of $\mathfrak{H}_{\mathfrak{p}}$ can appear in two different roles, either as differential operators on G (or $A_{\mathfrak{p}}$) or as polynomial functions on $\mathfrak{h}_{\mathfrak{p}}$. They should always be interpreted as differential operators unless some qualification to the contrary is made.

[23] Note that the constant function 1 is not included among the generators of $\mathfrak{R}$.

$$b - u - \sum_{1 \leqq i \leqq r} g_i(h) v_i \in \mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h^{-1}}\mathfrak{B}$$

for all $h \in A_{\mathfrak{p}}'$.

We shall use induction on d. Since $\mathfrak{g} = \mathfrak{k} + \mathfrak{h}_{\mathfrak{p}} + \theta(\mathfrak{n})$ and the sum is direct, it follows from [5(c), Lemma 12] that[11]

$$\mathfrak{B}_d = \sum_{p+q+r \leqq d}' \lambda(S_p(\theta(\mathfrak{n})))\lambda(S_q(\mathfrak{h}_{\mathfrak{p}}))\lambda(S_r(\mathfrak{k}))$$

where λ is the canonical mapping of $S(\mathfrak{g})$ onto $\mathfrak{B}$ and S_i refers to the space of homogeneous elements of degree i. Hence we can select $u \in \mathfrak{H}_{\mathfrak{p}} \cap \mathfrak{B}_d$ and $b_\beta \in \mathfrak{B}_{d-1}$ such that

$$b - u - \sum_{\beta \in P_+} \theta(X_\beta) b_\beta \in \mathfrak{B}\mathfrak{k}.$$

Now let $X_\beta = Y_\beta + Z_\beta$ $(Y_\beta \in \mathfrak{p}, Z_\beta \in \mathfrak{k})$. Then if $h \in A_{\mathfrak{p}}'$ and $H = \log h$,

$$\begin{aligned} \operatorname{Ad}(h^{-1})Z_\beta &= \tfrac{1}{2}(\operatorname{Ad}(h^{-1})X_\beta + \theta(\operatorname{Ad}(h)X_\beta)) \\ &= -\tfrac{1}{2}(e^{\beta(H)} - e^{-\beta(H)})Y_\beta + \tfrac{1}{2}(e^{\beta(H)} + e^{-\beta(H)})Z_\beta. \end{aligned}$$

Hence $Y_\beta \equiv (1 + 2g_\beta(h))Z_\beta \bmod \mathfrak{k}^{h^{-1}}$. Therefore since $\theta(X_\beta) = -Y_\beta + Z_\beta$, we get the following result which will be useful later on.

LEMMA 25. *For any* $\beta \in P_+$ *let* $X_\beta = Y_\beta + Z_\beta$ *where* $Y_\beta \in \mathfrak{p}$ *and* $Z_\beta \in \mathfrak{k}$. *Then* $\theta(X_\beta) \equiv -2g_\beta(h)Z_\beta \bmod \mathfrak{k}^{h^{-1}}$ *for* $h \in A_{\mathfrak{p}}'$.

This means that

$$b \equiv u - 2\sum_{\beta \in P_-} g_\beta(h)[Z_\beta, b_\beta] \bmod (\mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h^{-1}}\mathfrak{B})$$

for all $h \in A_{\mathfrak{p}}'$. But $[Z_\beta, b_\beta] \in \mathfrak{B}_{d-1}$ and so the assertion of Lemma 24 follows immediately by induction hypothesis.

Now it is obvious from the definition of $\delta_h'(b)$ that $\delta_h'(b) = u + \sum_{1 \leqq i \leqq r} g_i(h)v_i$ for $h \in A_{\mathfrak{p}}'$, in the notation of Lemma 24. Therefore since g_i are analytic functions on $A_{\mathfrak{p}}'$, $\delta'(b) = u + \sum_{1 \leqq i \leqq r} g_i v_i$ is an analytic differential operator on $A_{\mathfrak{p}}'$ whose local expression at h is $\delta_h'(b)$.

6. The relation between γ and δ. Let μ be a linear function on $\mathfrak{h}_{\mathfrak{p}}$. Then e^μ is a holomorphic function on the complex Euclidean space $\mathfrak{h}_{\mathfrak{p}}$. We agree to denote the function $h \to e^{\mu(\log h)}$ on $A_{\mathfrak{p}}$ also by e^μ. Now put[24] $\delta(b) = e^\rho \delta'(b) \circ e^{-\rho}$ $(b \in \mathfrak{B})$ where ρ is defined as in Section 4. The following lemma establishes a connection between $\delta(q)$ and $\gamma(q)$ for $q \in I_{\mathfrak{g}}$.

---

[24] Whenever it is necessary to avoid confusion we denote the operator product of two differential operators D, D' by $D \circ D'$. Since a function f of class C^∞ can also be regarded as a differential operator, one has to distinguish between Df and $D \circ f$.

LEMMA 26. *Let q be an element in $I_{\mathfrak{g}}$ of degree d. Then we can select a finite number of elements $v_i \in \mathfrak{H}_{\mathfrak{p}} \cap \mathfrak{B}_{d-1}$ and $g_i \in \mathfrak{R}$ $(1 \leqq i \leqq r)$ such that*

$$\delta(q) = \gamma(q) + \sum_{1 \leqq i \leqq r} g_i v_i$$

on $A_{\mathfrak{p}}'$.

We have seen in Section 4 that $I_{\mathfrak{g}} = I_{\mathfrak{g}} \cap \mathfrak{P} + I_{\mathfrak{g}} \cap \mathfrak{B}\mathfrak{k}$. Moreover it is easy to see that $\mathfrak{B}$ is the direct sum of $\mathfrak{P}$ and $\mathfrak{B}\mathfrak{k}$ and

$$\mathfrak{B}_d = (\mathfrak{B}_d \cap \mathfrak{P}) + (\mathfrak{B}_d \cap \mathfrak{B}\mathfrak{k}).$$

Therefore if q_1, q_2 are the components of q in $I_{\mathfrak{g}} \cap \mathfrak{P}$ and $I_{\mathfrak{g}} \cap \mathfrak{B}\mathfrak{k}$ respectively, they are both of degree $\leqq d$. Also $\delta(q_2) = 0$, $\gamma(q_2) = 0$ and every homogeneous component of q_1 lies in $I_{\mathfrak{g}} \cap \mathfrak{P}$. Hence it would clearly be sufficient to consider the case when $q \in I_{\mathfrak{g}} \cap \mathfrak{P}$.

Let $b \rightarrow b^*$ denote the anti-automorphism of $\mathfrak{B}$ given by $X^* = -X$ $(X \in \mathfrak{g})$. Then if p is a homogeneous polynomial in $S(\mathfrak{g})$ of degree r and λ the canonical mapping of $S(\mathfrak{g})$ into $\mathfrak{B}$, it is clear that $\lambda(p)^* = (-1)^r \lambda(p)$. But $X^* = \theta(X)$ for $X \in \mathfrak{p}$. Hence if we extend θ to an automorphism of $\mathfrak{B}$, it follows that $\theta(p) = p^*$ for $p \in \mathfrak{P}$. Let $\gamma'(q)$ denote the element in $\mathfrak{H}_{\mathfrak{p}}$ such that $q - \gamma'(q) \in \mathfrak{B}\mathfrak{n} + \mathfrak{k}\mathfrak{B}$ (see Lemma 3). Then $q^* - (\gamma'(q))^* \in \mathfrak{n}\mathfrak{B} + \mathfrak{B}\mathfrak{k}$ and therefore

$$q - \gamma'(q) = \theta(q^*) - \theta(\gamma'(q)^*) \in \theta(\mathfrak{n})\mathfrak{B} + \mathfrak{B}\mathfrak{k}.$$

Therefore we can select $b_\beta \in \mathfrak{B}_{d-1}$ such that

$$q - \gamma'(q) - \sum_{\beta \in P_+} \theta(X_\beta) b_\beta \in \mathfrak{B}\mathfrak{k}.$$

But then from Lemma 25,

$$q \equiv \gamma'(q) - \sum_{\beta \in P_+} g_\beta(h) b_\beta' \bmod (\mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h-1}\mathfrak{B})$$

for $h \in A_{\mathfrak{p}}'$ where $b_\beta' = 2[Z_\beta, b_\beta] \in \mathfrak{B}_{d-1}$. Therefore by Lemma 24 we can select a finite number of elements $v_i' \in \mathfrak{H}_{\mathfrak{p}} \cap \mathfrak{B}_{d-1}$ and $g_i \in \mathfrak{R}$ $(1 \leqq i \leqq r)$ such that

$$q \equiv \gamma'(q) + \sum_{1 \leqq i \leqq r} g_i(h) v_i' \bmod (\mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h-1}\mathfrak{B}) \qquad (h \in A_{\mathfrak{p}}').$$

But this means that $\delta'(q) = \gamma'(q) + \sum_i g_i v_i'$ and therefore

$$\delta(q) = \gamma(q) + \sum_{1 \leqq i \leqq r} g_i v_i$$

where [22] $v_i = e^{\rho} v_i' \circ e^{-\rho}$. Since it is obvious that $v_i \in \mathfrak{H}_{\mathfrak{p}}$, our assertion is proved.

Now select homogeneous elements $u_1 = 1, u_2, \cdots, u_w$ in $\mathfrak{H}_{\mathfrak{p}}$ in accordance with the corollary of Lemma 8, so that $\mathfrak{H}_\mathfrak{p} = \sum_{1 \leqq i \leqq w} Ju_i$ where $J = I(\mathfrak{h}_\mathfrak{p})$. We know from Theorem 1 that $\gamma(I_\mathfrak{g}) = J$.

THEOREM 2. *Let u be an element in $\mathfrak{H}_\mathfrak{p}$ and select $q_i \in I_\mathfrak{g}$ $(1 \leqq i \leqq w)$ such that $u = \sum_{1 \leqq i \leqq w} \gamma(q_i)u_i$. Then we can choose a finite number of elements $g_{ij} \in \mathfrak{R}$ and $q_{ij} \in I_\mathfrak{g}$ $(1 \leqq i \leqq w, 1 \leqq j \leqq r)$ such that*

$$u = \sum_{1 \leqq i \leqq w} u_i \circ \delta(q_i) + \sum_{1 \leqq i \leqq w} \sum_{1 \leqq j \leqq r} g_{ij} u_i \circ \delta(q_{ij})$$

on $A_\mathfrak{p}'$.

We shall use induction on the degree d of u. Obviously u can be assumed to be homogeneous. Put $I_\mathfrak{p} = I_\mathfrak{g} \cap \mathfrak{P}$. If we replace each q_i by its component in $I_\mathfrak{p}$ (with respect to the direct sum $\mathfrak{B} = \mathfrak{P} + \mathfrak{B}\mathfrak{k}$), neither $\gamma(q_i)$ nor $\delta(q_i)$ is affected. Hence we can suppose that $q_i \in I_\mathfrak{p}$. Let d_i denote the degree of u_i. Then it follows from our assumptions (see the corollary of Lemma 8) that $\gamma(q_i)$ is homogeneous of degree $d - d_i$ if $d \geqq d_i$ and $\gamma(q_i) = 0$ if $d_i > d$. Now fix i and first suppose $d \geqq d_i$. Then by Lemma 20, q_i is of degree $d - d_i$ and $\gamma(q_i)u_i = u_i \circ \delta(q_i) - u_i \circ (\delta(q_i) - \gamma(q_i))$ on $A_\mathfrak{p}'$. Since $\mathfrak{R}$ is stable under the operations of $\mathfrak{H}_\mathfrak{p}$, it follows from Lemma 26 that $u_i \circ (\delta(q_i) - \gamma(q_i)) = \sum_{1 \leqq j \leqq r} g_j v_j$ where $g_j \in \mathfrak{R}$ and $v_j \in \mathfrak{H}_\mathfrak{p} \cap \mathfrak{B}_{d-1}$. On the other hand if $d < d_i$, $\gamma(q_i) = 0$ and therefore $q_i = 0$ by Lemma 19. Hence $\gamma(q_i)u_i = u_i \circ \delta(q_i) = 0$ in this case. This shows that we can select a finite set of elements $g_j \in \mathfrak{R}$ and $v_j \in \mathfrak{H}_\mathfrak{p} \cap \mathfrak{B}_{d-1}$ $(1 \leqq j \leqq s)$ such that

$$u = \sum_{1 \leqq i \leqq w} u_i \circ \delta(q_i) + \sum_{1 \leqq j \leqq s} g_j v_j$$

on $A_\mathfrak{p}'$. The statement of the theorem now follows immediately by applying the induction hypothesis to v_j.

The following consequence of this theorem will be important for our applications.

COROLLARY. *Let U be a nonempty open connected subset of $A_\mathfrak{p}'$ and χ a homomorphism of $I_\mathfrak{g}$ into C. Let E_χ denote the space of all analytic functions ϕ on U which satisfy the system of differential equations $\delta(q)\phi = \chi(q)\phi$ $(q \in I_\mathfrak{g})$. Then the dimension of E_χ over C cannot exceed w.*

Choose a point h_0 in U. If $\dim E_\chi > w$, we can obviously find a function $\phi \neq 0$ in E_χ such that $\phi(h_0; u_i) = 0$ $(1 \leqq i \leqq w)$. But then it follows from the above theorem that $\phi(h_0; u) = 0$ for every $u \in \mathfrak{H}_\mathfrak{p}$. However since U is connected and ϕ is analytic, this implies that $\phi = 0$ and so we get a contradiction. Hence $\dim E_\chi \leqq w$.

7. The operator $\delta'(\omega)$. The Casimir operator ω of $\mathfrak{g}$ is an element lying in the center of $\mathfrak{B}$ which is defined as follows. Let $X_1, \cdots, X_n$ be a base for $\mathfrak{g}$ and put $g_{ij} = B(X_i, X_j)$ $1 \leqq i, j \leqq n$. Then the matrix $(g_{ij})_{1 \leqq i, j \leqq n}$ is nonsingular and if $(g^{ij})_{1 \leqq i, j \leqq n}$ denotes its inverse, $\omega = \sum_{1 \leqq i, j \leqq n} g^{ij} X_i X_j$. (It is easy to check that ω does not depend on the choice of the base used in its definition.) We intend to compute $\delta'(\omega)$.

For any linear function μ on $\mathfrak{h}_\mathfrak{p}$, let H_μ denote the unique element in $\mathfrak{h}_\mathfrak{p}$ such that $B(H, H_\mu) = \mu(H)$ for all $H \in \mathfrak{h}_\mathfrak{p}$. Also put $\gamma'(q) = e^{-\rho} \gamma(q) \circ e^{\rho}$ for $q \in I_\mathfrak{g}$.

LEMMA 27. $\delta'(\omega) = \gamma'(\omega) + 2 \sum_{\alpha \in P_+} (e^{2\bar{\alpha}} - 1)^{-1} H_{\bar{\alpha}}$ *where* $\bar{\alpha}$ *denotes the restriction of* α *on* $\mathfrak{h}_\mathfrak{p}$.

For each root α, select X_α as before and normalize it in such a way that $B(X_\alpha, X_{-\alpha}) = 1$ for any $\alpha \in P$. Then $[X_\alpha, X_{-\alpha}] = H_\alpha$ where H_α is the element in $\mathfrak{h}$ such that $B(H, H_\alpha) = \alpha(H)$ for every $H \in \mathfrak{h}$. Choose bases $H_1, \cdots, H_l$ and $H_{l+1}, \cdots, H_m$ for $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{h}_\mathfrak{k}$ respectively such that[9] $B(H_i, H_j) = \delta_{ij}$ $(1 \leqq i, j \leqq m)$. Then $H_1, \cdots, H_m$ together with X_α, $X_{-\alpha}$ $(\alpha \in P)$, form a base for $\mathfrak{g}$ and therefore it is clear that

$$\begin{aligned} \omega &= H_1^2 + \cdots + H_m^2 + \sum_{\alpha \in P} (X_\alpha X_{-\alpha} + X_{-\alpha} X_\alpha) \\ &= H_1^2 + \cdots + H_m^2 + 2 \sum_{\alpha \in P} X_{-\alpha} X_\alpha + \sum_{\alpha \in P} H_\alpha \\ &\equiv H_1^2 + \cdots + H_l^2 + 2H_\rho + 2 \sum_{\alpha \in P_+} X_{-\alpha} X_\alpha \bmod \mathfrak{k}\mathfrak{B} \cap \mathfrak{B}\mathfrak{k}, \end{aligned}$$

since X_α, $X_{-\alpha}$ and H_α lie in $\mathfrak{k}$ if α vanishes identically on $\mathfrak{h}_\mathfrak{p}$. This shows that $\omega \equiv H_1^2 + \cdots + H_l^2 + 2H_\rho \bmod (\mathfrak{k}\mathfrak{B} + \mathfrak{B}\mathfrak{n})$ and hence $\gamma'(\omega)$ $H_1^2 + \cdots + H_l^2 + 2H_\rho$. Now for any root α, which is not identically zero on $\mathfrak{h}_\mathfrak{p}$, let $X_\alpha = Y_\alpha + Z_\alpha$ $(Y_\alpha \in \mathfrak{p}, Z_\alpha \in \mathfrak{k})$ and put $g_\alpha(\exp H) = (e^{2\alpha(H)} - 1)^{-1}$ $(H \in \mathfrak{h}_{\mathfrak{p}_0}')$. We have seen in Section 5 that $Y_\alpha \equiv (1 + 2g_\alpha(h)) Z_\alpha \bmod \mathfrak{k}^{h^{-1}}$ for $h \in A_\mathfrak{p}'$. Hence

$$\begin{aligned} X_\alpha X_{-\alpha} \equiv X_\alpha Y_{-\alpha} &\equiv 2(1 + g_\alpha(h)) Z_\alpha Y_{-\alpha} \\ &\equiv 2(1 + g_\alpha(h)) [Z_\alpha, Y_{-\alpha}] \bmod (\mathfrak{k}^{h^{-1}} \mathfrak{B} + \mathfrak{B}\mathfrak{k}). \end{aligned}$$

If we apply the automorphism θ to this congruence, we get

$$\theta(X_\alpha X_{-\alpha}) \equiv -2(1 + g_\alpha(h)) [Z_\alpha, Y_{-\alpha}] \bmod (\mathfrak{k}^h \mathfrak{B} + \mathfrak{B}\mathfrak{k}).$$

Replacing α and h by $-\alpha$ and h^{-1} respectively, we find that

$$\theta(X_{-\alpha} X_\alpha) \equiv -2(1 + g_\alpha(h)) [Z_{-\alpha}, Y_\alpha] \bmod (\mathfrak{k}^{h^{-1}} \mathfrak{B} + \mathfrak{B}\mathfrak{k}).$$

This shows that

$$\tfrac{1}{2}\{X_\alpha X_{-\alpha} + \theta(X_{-\alpha}X_\alpha)\}$$
$$\equiv (1 + g_\alpha(h))\{[Z_\alpha, Y_{-\alpha}] - [Z_{-\alpha}, Y_\alpha]\} \bmod (\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k}).$$

But $[X_\alpha, X_{-\alpha}] = H_\alpha$ and therefore

$$[Z_\alpha, Y_{-\alpha}] + [Y_\alpha, Z_{-\alpha}] = \tfrac{1}{2}(H_\alpha - \theta(H_\alpha)) = H_\alpha.$$

This proves that

$$\tfrac{1}{2}\{X_\alpha X_{-\alpha} + \theta(X_{-\alpha}X_\alpha)\} \equiv (1 + g_\alpha(h))H_{\bar{\alpha}} \bmod (\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k})$$

for $h \in A_{\mathfrak{p}}'$. On the other hand it is easy to verify that $\theta(\omega) = \omega$. Therefore

$$\omega = \tfrac{1}{2}\{\omega + \theta(\omega)\}$$
$$\equiv (H_1^2 + \cdots + H_l^2) + \tfrac{1}{2}\sum_{\alpha \in P_+}\{X_\alpha X_{-\alpha} + X_{-\alpha}X_\alpha$$
$$+ \theta(X_\alpha X_{-\alpha} + X_{-\alpha}X_\alpha)\} \bmod \mathfrak{B}\mathfrak{k}.$$

But in view of the above result, this implies that

$$\omega \equiv (H_1^2 + \cdots + H_l^2) + \sum_{\alpha \in P_+}(1 + 2g_\alpha(h))H_{\bar{\alpha}} \bmod (\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k})$$

since $g_\alpha - g_{-\alpha} = 1 + 2g_\alpha$. Hence

$$\omega \equiv \gamma'(\omega) + 2\sum_{\alpha \in P_+} g_\alpha(h)H_{\bar{\alpha}} \bmod (\mathfrak{k}^{h^{-1}}\mathfrak{B} + \mathfrak{B}\mathfrak{k})$$

for $h \in A_{\mathfrak{p}}'$ and this proves the lemma.

COROLLARY 1. *Let $H_1, \cdots, H_l$ be any base for $\mathfrak{h}_{\mathfrak{p}}$ and let $(g^{ij})_{1 \leqq i,j \leqq l}$ denote the inverse of the matrix $g_{ij} = B(H_i, H_j)$ $(1 \leqq i, j \leqq l)$. Then*

$$\delta'(\omega) = \Delta^{-1}\sum_{1 \leqq i,j \leqq l} g^{ij}H_i \circ \Delta H_j.$$

It is easy to check that the right side is actually independent of the choice of the base $H_1, \cdots, H_l$. Hence it is sufficient to consider the base used in the proof of the above lemma. But then one finds by direct calculation that

$$\Delta^{-1}\sum_{1 \leqq i,j \leqq l} g^{ij}H_i \circ \Delta H_j = (H_1^2 + \cdots + H_l^2) + \sum_{\alpha \in P_+}\{(e^{\bar{\alpha}} + e^{-\bar{\alpha}})/(e^{\bar{\alpha}} - e^{-\bar{\alpha}})\}H_{\bar{\alpha}}$$
$$= \gamma'(\omega) + 2\sum_{\alpha \in P_+}(e^{2\bar{\alpha}} - 1)^{-1}H_{\bar{\alpha}}$$

and this proves our assertion.

Let ϖ denote the restriction on $\mathfrak{h}_{\mathfrak{p}}$ of the Casimir polynomial of $\mathfrak{g}$ (see [5(k), p. 98]).

COROLLARY 2. $\gamma(\omega)=\varpi-\langle\rho,\rho\rangle$.

We keep to the notation of the proof of Lemma 27. Since $\gamma'(\omega) = (H_1^2+\cdots+H_l^2)+2H_\rho$ it is clear that

$$\begin{aligned}\gamma(\omega) &= (H_1^2+\cdots+H_l^2)-2\sum_{1\leqq i\leqq l}\rho(H_i)H_i+\langle\rho,\rho\rangle+2(H_\rho-\langle\rho,\rho\rangle)\\ &= (H_1^2+\cdots+H_l^2)-\langle\rho,\rho\rangle.\end{aligned}$$

On the other hand $\varpi=H_1^2+\cdots+H_l^2$ and so our assertion is obvious.

8. **Some consequences of Lemma 27.** Select $\alpha_1,\cdots,\alpha_l\in\Sigma$ as in Section 3 and let L denote the set of all linear functions on $\mathfrak{h}_\mathfrak{p}$ of the form $m_1\alpha_1+\cdots+m_l\alpha_l$ where $m_1,\cdots,m_l$ are nonnegative integers. Given two linear functions λ,λ' on $\mathfrak{h}_\mathfrak{p}$, we write $\lambda<<\lambda'$ (or $\lambda'>>\lambda$) if $\lambda\neq\lambda'$ and $\lambda'-\lambda\in L$. It is clear that for any two linear functions λ_1,λ_2 on $\mathfrak{h}_\mathfrak{p}$, there exist only a finite number of λ such that $\lambda_1<<\lambda<<\lambda_2$. Define $S=S(\mathfrak{h}_\mathfrak{p})$ as in Section 3 and let $Q=Q(\mathfrak{h}_\mathfrak{p})$ denote the quotient field of S. Then Q is the field of rational functions on $\mathfrak{h}_\mathfrak{p}$. Introduce the scalar product $\langle p,q\rangle$ for $p,q\in S$ as in [5(k), p. 90] and put $m(\lambda)=m_1+\cdots+m_l$ for $\lambda=m_1\alpha_1+\cdots+m_l\alpha_l\in L$. Now for each $\lambda\in L$, we define an element ${}'\Gamma_\lambda\in Q$ by induction on $m(\lambda)$ as follows. ${}'\Gamma_0=1$ and[25]

$$\{\langle\lambda,\lambda-2\rho\rangle-2\lambda\}{}'\Gamma_\lambda=2\sum_{\alpha\in P_+}\sum_{k\geqq 1}{}'\Gamma_{\lambda-2k\bar{\alpha}}\{\langle\lambda-2k\bar{\alpha},\bar{\alpha}\rangle-\bar{\alpha}\},$$

where $\bar{\alpha}$ denotes the restriction of α on $\mathfrak{h}_\mathfrak{p}$ and k runs over all positive integers such that $\lambda-2k\bar{\alpha}\in L$. Let L' denote the set of all elements $\lambda\neq 0$ in L. Consider the hyperplane σ_λ' ($\lambda\in L'$) consisting of those points $H\in\mathfrak{h}_\mathfrak{p}$ where $2\lambda(H)=\langle\lambda,\lambda-2\rho\rangle$. It is clear that any compact subset of $\mathfrak{h}_\mathfrak{p}$ meets σ_λ' for only a finite number of λ in L'. Let $\mathfrak{h}_\mathfrak{p}''$ denote the complement of $\bigcup_{\lambda\in L'}\sigma_\lambda'$ in $\mathfrak{h}_\mathfrak{p}$. Then $\mathfrak{h}_\mathfrak{p}''$ is an open, connected, dense subset of $\mathfrak{h}_\mathfrak{p}$. It is obvious that the rational function ${}'\Gamma_\lambda$ ($\lambda\in L$) takes a well-defined value at any point $H\in\mathfrak{h}_\mathfrak{p}''$. We denote this value by ${}'\Gamma_\lambda(H)$.

LEMMA 28. *Let U be a compact subset of $\mathfrak{h}_\mathfrak{p}''$. Then there exists a real number $c\geqq 1$ such that $|{}'\Gamma_\lambda(H)|\leqq c^{m(\lambda)}$ for $\lambda\in L$ and $H\in U$.*

Select positive numbers c_1 and c_2 such that

$$|\langle\lambda,\bar{\alpha}\rangle-\alpha(H)|\leqq c_1(m(\lambda)+1),\qquad |\langle\lambda,\lambda-2\rho\rangle-2\lambda(H)|\geqq c_2m(\lambda)^2$$

---

[25] As will become apparent during the proof of Lemma 29, the motivation for this definition comes from Lemma 27.

for every $\lambda \in L$, $\alpha \in P_+$ and $H \in U$. Obviously this is possible. Now if $\lambda' << \lambda$ $(\lambda' \in L)$, it is clear that $m(\lambda') < m(\lambda)$ and therefore

$$|\langle \lambda, \bar{\alpha} \rangle - \alpha(H)| \, |\langle \lambda, \lambda - 2\rho \rangle - 2\lambda(H)|^{-1} \leqq c_3/m(\lambda) \qquad (H \in U)$$

where $c_3 = 2c_1/c_2$. Hence it follows that

$$|{}'\Gamma_\lambda(H)| \leqq 2c_3(m(\lambda))^{-1} \sum_{\alpha \in P_+} \sum_{k \geqq 1} |{}'\Gamma_{\lambda - 2k\bar{\alpha}}(H)| \qquad (H \in U, \lambda \in L').$$

Let r be the number of roots in P_+ and put $c = \max\{rc_3, 1\}$. We shall prove by induction on $m(\lambda)$ that $|{}'\Gamma_\lambda(H)| \leqq c^{m(\lambda)}$ for $H \in U$ and $\lambda \in L$. If $\lambda = 0$, this is true. So now suppose $\lambda \neq 0$. Since $\lambda - 2k\bar{\alpha} \in L$, it is obvious that $k \leqq \frac{1}{2}m(\lambda)$. Hence it follows by induction hypothesis that

$$\sum_{k \geqq 1} |{}'\Gamma_{\lambda - 2k\bar{\alpha}}(H)| \leqq \tfrac{1}{2}m(\lambda) c^{m(\lambda)-1}$$

and therefore

$$|{}'\Gamma_\lambda(H)| \leqq c_3 r c^{m(\lambda)-1} \leqq c^{m(\lambda)}$$

For any number $M \geqq 0$, let $\mathfrak{h}_\mathfrak{p}(M)$ denote the set of those points $H \in \mathfrak{h}_\mathfrak{p}$ where the real part of $\alpha_i(H)$ is greater than M for every i $(1 \leqq i \leqq l)$.

COROLLARY 1. *We can choose* $M \geqq 0$ *such that the series*

$$\sum_{\lambda \in L} |{}'\Gamma_\lambda(H') e^{-\lambda(H)}|$$

converges uniformly for $H \in \mathfrak{h}_\mathfrak{p}(M)$ *and* $H' \in U$.

Obviously it is sufficient to choose M so large that $c < e^M$.

COROLLARY 2. *Let* U' *be an open subset of* $\mathfrak{h}_\mathfrak{p}''$ *whose closure (in* $\mathfrak{h}_\mathfrak{p}''$*) is compact. Then if* M *is sufficiently large, the function* $\phi'(H' : H)$ $(H' \in U'$, $H \in \mathfrak{h}_\mathfrak{p}(M))$ *defined by the series*

$$\phi'(H' : H) = e^{\langle H', H \rangle} \sum_{\lambda \in L} {}'\Gamma_\lambda(H') e^{-\lambda(H)}$$

is holomorphic on $U' \times \mathfrak{h}_\mathfrak{p}(M)$.

This is an immediate consequence of Corollary 1.

We keep to the notation of Corollary 2 above and denote by $A_\mathfrak{p}(M)$ the set of those points $h \in A_\mathfrak{p}$ for which $\log h \in \mathfrak{h}_\mathfrak{p}(M)$. Also put $\Phi'(H' : h) = \phi'(H' : \log h)$ $(H' \in U', h \in A_\mathfrak{p}(M))$. Then Φ' is an analytic function on $U' \times A_\mathfrak{p}(M)$. The following lemma provides the justification for the above construction.

LEMMA 29. *Let* q *be an element in* $I_\mathfrak{g}$. *Then*[11]

$$\Phi'(H' : h ; \delta'(q)) = \gamma'(q : H') \Phi'(H' : h) \qquad (H' \in U, h \in A_\mathfrak{p}(M))$$

where $\gamma'(q : H')$ *denotes the value of the polynomial function*[26] $\gamma'(q)$ *at* H'.

---

[26] We recall that $\gamma'(q) = e^{-\rho}\gamma(q) \circ e^{\rho}$.

For otherwise suppose our assertion is false. Then from Lemma 26, $\delta'(q) = \gamma'(q) + \sum_{1 \leqq i \leqq r} g_i v_i$ where $g_i \in \mathfrak{R}$ and $v_i \in \mathfrak{H}_{\mathfrak{p}}$. For any $v \in S(\mathfrak{h}_{\mathfrak{p}})$, let $\partial(v)$ denote the corresponding differential operator on $\mathfrak{h}_{\mathfrak{p}}$ (see [5(k), § 2]). Then if ψ is a holomorphic function on $\mathfrak{h}_{\mathfrak{p}}(M)$ and $\Psi(h) = \psi(\log h)$ $(h \in A_{\mathfrak{p}}(M))$, it is obvious that $\Psi(h; v) = \psi(\log h; \partial(v))$ for $v \in \mathfrak{H}_{\mathfrak{p}}$. Therefore in particular

$$\Psi(h; \sum_{1 \leqq i \leqq r} g_i v_i) = \sum_{1 \leqq i \leqq r} g_i(h) \psi(\log h; \partial(v_i)).$$

But $g_\alpha(\exp H) = (e^{2\alpha(H)} - 1)^{-1} = \sum_{1 \leqq k < \infty} e^{-2k\alpha(H)}$ for $\alpha \in P_+$ and $H \in \mathfrak{h}_{\mathfrak{p}}(M)$. Hence it is obvious that we can select an element $v_\lambda \in \mathfrak{H}_{\mathfrak{p}}$ for each $\lambda \in L'$, such that

$$\sum_{1 \leqq i \leqq r} g_i(\exp H) \psi(H; \partial(v_i)) = \sum_{\lambda \in L'} e^{-\lambda(H)} \psi(H; \partial(v_\lambda)) \qquad (H \in \mathfrak{h}_{\mathfrak{p}}(M))$$

for any holomorphic function ψ on $\mathfrak{h}_{\mathfrak{p}}(M)$. Hence in particular

$$\Phi'(H' : h; \delta'(q)) - \gamma'(q : H') \Phi'(H' : h) = \phi_1(H' : \log h) \qquad (h \in A_{\mathfrak{p}}(M))$$

where

$$\phi_1(H' : H) = \phi'(H' : H; \partial(\gamma'(q)) - \gamma'(q : H')) + \sum_{\lambda \in L'} e^{-\lambda(H)} \phi'(H' : H; \partial(v_\lambda))$$

for $H' \in U'$ and $H \in \mathfrak{h}_{\mathfrak{p}}(M)$. Now put $\phi_0(H' : H) = e^{-\langle H', H \rangle} \phi_1(H' : H)$. Then it follows from our hypothesis that $\phi_0 \neq 0$. On the other hand it is obvious that

$$\phi'(H' : H; \partial(v)) = e^{\langle H', H \rangle} \sum_{\lambda \in L} {}'\Gamma_\lambda(H') v(H' - H_\lambda) e^{-\lambda(H)}$$
$$(H' \in U', H \in \mathfrak{h}_{\mathfrak{p}}(M))$$

for $v \in \mathfrak{H}_{\mathfrak{p}}$. (Here $v(H' - H_\lambda)$ denotes the value of the polynomial function v and $H' - H_\lambda$.) Hence

$$\begin{aligned} \phi_0(H' : H) &= \sum_{\lambda \in L} {}'\Gamma_\lambda(H') e^{-\lambda(H)} \{\gamma'(q : H' - H_\lambda) - \gamma'(q : H')\} \\ &\quad + \sum_{\lambda \in L} \sum_{\mu \in L'} {}'\Gamma_\lambda(H') e^{-\lambda(H) - \mu(H)} v_\mu(H' - H_\lambda) \\ &= \sum_{\lambda \in L} e^{-\lambda(H)} c_\lambda(H') \end{aligned}$$

where

$$c_\lambda(H') = {}'\Gamma_\lambda(H') \{\gamma'(q : H' - H_\lambda) - \gamma'(q : H')\}$$
$$+ \sum_{0 \ll \mu \ll \lambda} {}'\Gamma_\mu(H') v_{\lambda - \mu}(H' - H_\mu).$$

Obviously c_λ is a rational function on $\mathfrak{h}_{\mathfrak{p}}$ and since $\phi_0 \neq 0$, we can choose $\lambda_0 \in L$ such that $c_{\lambda_0} \neq 0$. We shall now show that this is actually impossible.

Let π be an irreducible representation of $\mathfrak{g}$ on a finite-dimensional space V_0. We assume that there exists a unit vector ξ in V_0 such that $\pi(\mathfrak{k})\xi = \{0\}$. As usual, we denote the corresponding representation of G_c also by π and put $\Xi(x) = (\xi, \pi(x)\xi)$ $(x \in G_c)$. Then Ξ is a holomorphic function on G_c. Let $\Lambda_1' > \Lambda_2' > \cdots > \Lambda_s'$ be all the weights of π and $\Lambda = \Lambda_1 > \Lambda_2 > \cdots > \Lambda_r$ all the linear functions on $\mathfrak{h}_{\mathfrak{p}}$ obtained by taking the restrictions of these weights on $\mathfrak{h}_{\mathfrak{p}}$. Then we know from [5(h), Lemma 2] that $\Lambda_i << \Lambda$ $(2 \leqq i \leqq r)$. Let V_i be the subspace consisting of those elements $\eta \in V_0$ for which $\pi(H)\eta = \Lambda_i(H)\eta$ $(H \in \mathfrak{h}_{\mathfrak{p}})$ and let E_i denote the orthogonal projection of V_0 on V_i. Then since $\pi(H)$ is self-adjoint for H in $\mathfrak{h}_{\mathfrak{p}_0}$, it follows that $V_1, \cdots, V_r$ are mutually orthogonal and therefore

$$\Xi(\exp H) = \sum_{1 \leqq i \leqq r} |E_i\xi|^2 e^{\Lambda_i(H)} \qquad (H \in \mathfrak{h}_{\mathfrak{p}}).$$

On the other hand put $E = \int_K \pi(k)\,dk$ and let η be a unit vector in V_0 belonging to the highest weight Λ_1'. Then we have seen during the proof of Lemma 5 that $\xi = cE\eta$ where c is a nonzero complex number. This shows that $(\xi, \eta) = (E\xi, \eta) = (\xi, E\eta) = c^{-1} \neq 0$. But $\eta \in V_1$ and therefore $(\xi, \eta) = (\xi, E_1\eta) = (E_1\xi, \eta)$. Hence $E_1\xi \neq 0$ and so

$$\Xi(\exp H) = \sum_{1 \leqq i \leqq r} a_i' e^{\Lambda_i(H)} \qquad (H \in \mathfrak{h}_{\mathfrak{p}})$$

where $a_1' = |E_1\xi|^2 > 0$ and $a_i' = |E_i\xi|^2 \geqq 0$ $(2 \leqq i \leqq r)$.

Let Ξ_0 denote the restriction of Ξ on G. Then Ξ_0 is a spherical function and therefore $\Xi_0(h; b) = \Xi_0(h; \delta'(b))$ $(b \in \mathfrak{B}, h \in A_{\mathfrak{p}}')$ by Lemma 23. Moreover if $b \in I_{\mathfrak{g}}$, it follows from Lemmas 3 and 5 that $b\Xi_0 = \gamma'(b : H_\Lambda)\Xi_0$. Therefore

$$\Xi_0(h; \delta'(b)) - \gamma'(b : H_\Lambda)\Xi_0(h) = 0 \qquad (b \in I_{\mathfrak{g}}; h \in A_{\mathfrak{p}}').$$

Now put $\Xi_1(H) = (a_1')^{-1} e^{-\Lambda(H)} \Xi(\exp H)$ and $\Xi_1'(H) = \Xi(\exp H)$ $(H \in \mathfrak{h}_{\mathfrak{p}})$. Then Ξ_1 can be written in the form

$$\Xi_1(H) = 1 + \sum_{\lambda \in L'} a_\lambda e^{-\lambda(H)} \qquad (H \in \mathfrak{h}_{\mathfrak{p}})$$

where a_λ are real numbers which are zero for all λ in L' except a finite number. Then by applying the above relation for $b = \omega$ and making use of Lemma 27, we find that

$$\begin{aligned}\Xi_1'(H; \partial(\gamma'(\omega))) + 2 \sum_{\alpha \in P_+} \sum_{1 \leqq k < \infty} e^{-2k\alpha(H)} \Xi_1'(H; \partial(H_{\bar{\alpha}})) \\ = \gamma'(\omega : H_\Lambda)\Xi_1'(H) \qquad (H \in \mathfrak{h}_{\mathfrak{p}}(M)).\end{aligned}$$

Hence if $a_0 = 1$,

$$\sum_{\lambda \in L} a_\lambda \gamma'(\omega : H_\Lambda - H_\lambda) e^{-\lambda(H)} + 2 \sum_{\alpha \in P_+} \sum_{1 \leqq k < \infty} e^{-2k\alpha(H)} \sum_{\lambda \in L} e^{-\lambda(H)} a_\lambda \langle \bar{\alpha}, \Lambda - \lambda \rangle$$
$$= \gamma'(\omega : H_\Lambda) \sum_{\lambda \in L} a_\lambda e^{-\lambda(H)} \qquad (H \in \mathfrak{h}_{\mathfrak{p}}(M)).$$

But $\gamma'(\omega : H) = \langle H, H \rangle + 2\rho(H)$ $(H \in \mathfrak{h}_{\mathfrak{p}})$ from Corollary 2 to Lemma 27. Therefore if $E(M)$ stands for the set of all points $H \in \mathfrak{h}_{\mathfrak{p}}(2M)$ where[27] $\operatorname{Re} \alpha_i(H) > \frac{1}{2} | \alpha_j(H) |$ $(1 \leqq i, j \leqq l)$, it follows by applying the corollary of Lemma 57 of the Appendix (§ 15) to $V = E(M)$ that we can equate the coefficients of $e^{-\lambda}$ on both sides of the above equation and obtain

$$a_\lambda \langle \Lambda - \lambda, \Lambda - \lambda + 2\rho \rangle + 2 \sum_{\alpha \in P_+} \sum_{k \geqq 1} a_{\lambda - 2k\bar{\alpha}} \langle \bar{\alpha}, \Lambda - \lambda + 2k\bar{\alpha} \rangle$$
$$= a_\lambda \langle \Lambda, \Lambda + 2\rho \rangle \qquad (\lambda \in L).$$

Here the sum is to be taken over those positive integers k for which $\lambda - 2k\bar{\alpha} \in L$. This proves that

$$\{ \langle \lambda, \lambda - 2\rho \rangle - 2\lambda(H_\Lambda) \} a_\lambda$$
$$= 2 \sum_{\alpha \in P_+} \sum_{k \geqq 1} a_{\lambda - 2k\bar{\alpha}} \{ \langle \lambda - 2k\bar{\alpha}, \bar{\alpha} \rangle - \bar{\alpha}(H_\Lambda) \}.$$

By comparing this with the recurrence relation for $'\Gamma_\lambda$, it is obvious that $a_\lambda = {'\Gamma_\lambda}(H_\Lambda)$ provided $H_\Lambda \notin \sigma_\mu'$ for any $\mu \in L'$ such that $\lambda - \mu \in L$. On the other hand it is clear from Lemma 4 that π can be selected in such a way that (1) $H_\Lambda \notin \sigma_\mu'$ for $\mu = \lambda_0$ or $\mu << \lambda_0$ $(\mu \in L')$ and (2) the rational function c_{λ_0} (which is then obviously defined at H_Λ) does not take the value zero at H_Λ. However the relation

$$\Xi_0(h ; \delta'(q)) - \gamma'(q : H_\Lambda) \Xi_0(h) = 0 \qquad (h \in A_{\mathfrak{p}}')$$

implies that

$$\sum_{\lambda \in L} a_\lambda e^{-\lambda(H)} \{ \gamma'(q : H_\Lambda - H_\lambda) - \gamma'(q : H_\Lambda) \}$$
$$+ \sum_{\lambda \in L} \sum_{\mu \in L'} a_\lambda e^{-\lambda(H) - \mu(H)} v_\mu (H_\Lambda - H_\lambda) = 0$$

for $H \in \mathfrak{h}_{\mathfrak{p}_0}(M) = \mathfrak{h}_{\mathfrak{p}_0} \cap \mathfrak{h}_{\mathfrak{p}}(M)$. Again by applying the corollary of Lemma 57 to $V = \mathfrak{h}_{\mathfrak{p}_0} \cap E(M)$, we can equate the coefficient of $e^{-\lambda}$ in the above expression, to zero. But it is obvious that this coefficient is $c_\lambda(H_\Lambda)$ for $\lambda = \lambda_0$ or $\lambda << \lambda_0$ $(\lambda \in L)$. Hence $c_{\lambda_0}(H_\Lambda) = 0$ and so we get a contradiction. This completes the proof of Lemma 29.

Let τ denote the mapping of $\mathfrak{h}_{\mathfrak{p}}$ into itself given by

$$\tau(H) = -(-1)^{\frac{1}{2}}(H + H_\rho) \qquad (H \in \mathfrak{h}_{\mathfrak{p}}).$$

---

[27] For any complex number c, $\operatorname{Re} c$ and $\operatorname{Im} c$ denote the real parts of c and $-(-1)^{\frac{1}{2}} c$ respectively.

Then $\tau^{-1}(H) = (-1)^{\frac{1}{2}}H - H_\rho$. For any polynomial $p \in S(\mathfrak{h}_{\mathfrak{p}})$, let p^τ denote the function whose value at $H \in \mathfrak{h}_{\mathfrak{p}}$ is $p(\tau^{-1}(H))$. Then the mapping $p \rightarrow p^\tau$ can be extended to an automorphism of $Q(\mathfrak{h}_{\mathfrak{p}})$. It is clear that a rational function $p \in Q(\mathfrak{h}_{\mathfrak{p}})$ is defined at a point H if and only if p^τ is defined at $\tau(H)$ and if this is so, $p(H) = p^\tau(\tau(H))$. Put $\sigma_\lambda = \tau(\sigma_\lambda')$ $(\lambda \in L')$ and ${}'\mathfrak{h}_{\mathfrak{p}} = \tau(\mathfrak{h}_{\mathfrak{p}}'')$. Then σ_λ consists of those points $H \in \mathfrak{h}_{\mathfrak{p}}$ where $\langle\lambda,\lambda\rangle = 2(-1)^{\frac{1}{2}}\lambda(H)$. This shows that $\mathfrak{h}_{\mathfrak{p}_0} \subset {}'\mathfrak{h}_{\mathfrak{p}}$. Put $\Gamma_\lambda = ({}'\Gamma_\lambda)^\tau$ $(\lambda \in L)$, $U = \tau(U')$ and

$$\phi(H_0 : H) = e^{\rho(H)}\phi'(\tau^{-1}(H_0) : H) = e^{(-1)^{\frac{1}{2}}\langle H_0, H\rangle} \sum_{\lambda \in L} \Gamma_\lambda(H_0) e^{-\lambda(H)}$$

for $H_0 \in U$ and $H \in \mathfrak{h}_{\mathfrak{p}}(M)$ (in the notation of Corollary 2 to Lemma 28). Moreover let

$$\Phi(H : h) = e^{\rho(\log h)}\Phi'(\tau^{-1}(H) : h) \qquad (H \in U, h \in A_{\mathfrak{p}}(M)).$$

Then Lemma 29 can be restated as follows.

Lemma 30. *For any q in $I_{\mathfrak{g}}$,*

$$\Phi(H : h; \delta(q)) = \gamma(q : (-1)^{\frac{1}{2}}H)\Phi(H : h)$$

if $H \in U$ and $h \in A_{\mathfrak{p}}(M)$.

Now put $\xi_\lambda(H_0 : H) = \exp\{(-1)^{\frac{1}{2}}\langle H_0, H\rangle - \lambda(H)\}\Gamma_\lambda(H_0)$ for $H_0 \in {}'\mathfrak{h}_{\mathfrak{p}}$, $H \in \mathfrak{h}_{\mathfrak{p}}$ and $\lambda \in L$. Then if $u \in S(\mathfrak{h}_{\mathfrak{p}})$, it follows from the uniform convergence (see Corollary 1 to Lemma 28) of the series $\sum_{\lambda \in L} |\xi_\lambda(H_0 : H)|$ on any compact subset Ω of $U \times \mathfrak{h}_{\mathfrak{p}}(M)$, that the series[11] $\sum_{\lambda \in L} \xi_\lambda(H_0; \partial(u) : H)$ also converges uniformly on Ω to $\phi(H_0; \partial(u) : H)$ (see Lemma 58 of the Appendix). Define $E(M)$ as above to be the set of all points $H \in \mathfrak{h}_{\mathfrak{p}}(2M)$ such that $\operatorname{Re} \alpha_i(H) > \frac{1}{2} |\alpha_j(H)|$ $(1 \leqq i, j \leqq l)$. Then if M is sufficiently large we have the following lemma.

Lemma 31. *Let U_1 be a compact subset of U. Then for any linear function μ on $\mathfrak{h}_{\mathfrak{p}}$ and $u \in S(\mathfrak{h}_{\mathfrak{p}})$, the series*

$$\sum_{\lambda \in L} |\xi_\lambda(H_0; \partial(u) : H) e^{\mu(H)}|$$

converges uniformly for $H_0 \in U_1$ and $H \in E(M)$.

In view of Lemma 58 of the Appendix, it is sufficient to show that the series $\sum_{\lambda \in L} |\xi_\lambda(H_0 : H) e^{\mu(H)}|$ converges uniformly for $H_0 \in U$ and $H \in E(M)$. Since the closure of U is compact, we can find a real number ν such that

$$|\exp\{(-1)^{\frac{1}{2}}\langle H_0, H\rangle + \mu(H)\} \leqq \exp\{\nu \operatorname{Re}(\alpha_1(H) + \cdots + \alpha_l(H))\}$$

for all $H_0 \in U$ and $H \in E(M)$. Let $\beta(H) = \min\limits_{1 \leqq i \leqq l} \operatorname{Re} \alpha_i(H)$. Then if $H \in E(M)$, $\operatorname{Re}(\alpha_1(H) + \cdots + \alpha_l(H)) \leqq 2l\beta(H)$ and $\operatorname{Re} \lambda(H) \geqq m(\lambda)\beta(H)$ $(\lambda \in L)$. Hence $|\xi_\lambda(H_0 : H) e^{\mu(H)}| \leqq |\Gamma_\lambda(H_0)| \exp\{(2\nu l - m(\lambda))2M\}$. Therefore if $m(\lambda) \geqq 4\nu l$,

$$|\xi_\lambda(H_0 : H) e^{\mu(H)}| \leqq |\Gamma_\lambda(H_0)| \exp(-m(\lambda)M)$$

and our assertion follows from Lemma 28.

Now fix an element $H_0 \in U$. We now use the notation of Section 3 and define W' and J' corresponding to the element H_0. Let V_{H_0} denote the subspace consisting of those elements $v \in S$ which satisfy the condition that $p(H_0; \partial(v)) = 0$ for every polynomial function $p \in SJ_{H_0}'$. Also let J_+' be the subspace spanned by homogeneous elements in J' of positive degree.

Lemma 32. *$S = V_{H_0} + SJ_+'$ and* $\dim V_{H_0} = w'$.

Put $V = V_{H_0}$ and let $p \to p^\sigma$ $(p \in S)$ denote the automorphism of S defined by $p^\sigma(H) = p(H + H_0)$ $(H \in \mathfrak{h}_{\mathfrak{p}})$. Since H_0 is left fixed by W', it is clear that $(J')^\sigma = J'$. Moreover p vanishes at H_0 if and only if p^σ vanishes at zero. Hence $(J_{H_0}')^\sigma = J_+'$. Also it is obvious that $(\partial(H)p)^\sigma = \partial(H)p^\sigma$ $(H \in \mathfrak{h}_{\mathfrak{p}}, p \in S)$ and therefore $(\partial(u)p)^\sigma = \partial(u)p^\sigma$ $(u \in S)$. This shows that V is exactly the set of those elements $v \in S$ which satisfy the condition $\langle v, p \rangle = 0$ for all $p \in SJ_+'$. For any $p \in S$, let p_* denote the polynomial function on $\mathfrak{h}_{\mathfrak{p}}$ given by $p_*(H) = \operatorname{conj} p(H)$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$. Then $\langle p, p_* \rangle$ is a positive-definite Hermitian form on S (see [5(k), p. 110]) and since J_+' is invariant under the mapping $p \to p_*$, V is the orthogonal complement of SJ_+' in S under this form. Hence $V \cap SJ_+' = \{0\}$. Moreover if S_d denotes the space of homogeneous elements in S of degree d, it is clear that $V \cap S_d$ is the orthogonal complement of $S_d \cap SJ_+'$ in S_d. Therefore since $\dim S_d$ is finite, it follows that $S_d = V \cap S_d + S_d \cap SJ_+'$ and so $S = V + SJ_+'$. But then $\dim V = \dim S/SJ_+' = w'$ from Lemma 13.

Corollary. *Suppose $v \in V_{H_0}$ and $q \in I_{\mathfrak{g}}$. Then*

$$\Phi(H_0; \partial(v) : h; \delta(q)) = \gamma(q : (-1)^{\frac{1}{2}} H_0) \Phi(H_0; \partial(v) : h)$$

for $h \in A_{\mathfrak{p}}(M)$.

Let p denote the polynomial function $H \to \gamma(q : (-1)^{\frac{1}{2}} H)$ on $\mathfrak{h}_{\mathfrak{p}}$ and let $(\partial(v) \circ p)_H$ denote the local expression (see [5(k), p. 90]) at $H \in \mathfrak{h}_{\mathfrak{p}}$ of the differential operator[24] $\partial(v) \circ p$ on $\mathfrak{h}_{\mathfrak{p}}$. We know from Lemma 30 that

$$\Phi(H : h; \delta(q)) = p(H) \Phi(H : h) \qquad (H \in U, h \in A_{\mathfrak{p}}(M))$$

and therefore it is obvious that

$$\Phi(H;\partial(v):h;\delta(q)) = \Phi(H;(\partial(v)\circ p)_H:h)$$

Hence it would be sufficient to prove that $(\partial(v)\circ p)_{H_0} = p(H_0)\partial(v)$. So let us suppose that $D = (\partial(v)\circ p)_{H_0} - p(H_0)\partial(v) \neq 0$. Then we can choose $p_1 \in S$ such that $p_1(H_0;D) \neq 0$. Put $p_2 = (p - p(H_0))p_1$. Then $p_1(H_0;D) = p_2(H_0;\partial(v))$. On the other hand $p \in J$ and therefore $p - p(H_0) \in J_{H_0}'$ and $p_2 \in SJ_{H_0}'$. But since $v \in V_{H_0}$, this implies that $p_2(H_0;\partial(v)) = 0$. Hence we get a contradiction and so the corollary is proved.

Put $r = [W:W']$ and select $s_1 = 1, s_2, \cdots, s_r$ in W such that $W = \bigcup_{1\leqq i\leqq r} s_iW'$. Then the points $H_i = s_iH_0$ $(1\leqq i\leqq r)$ are all distinct. We assume that $H_i \in {}'\mathfrak{h}_\mathfrak{p}$ $1\leqq i\leqq r$ and $(-1)^{\frac{1}{2}}(H_i - H_j)$, regarded as a linear function on $\mathfrak{h}_\mathfrak{p}$, does not lie in L for any pair of indices $i\neq j$ $(1\leqq i,j\leqq r)$. Put $V_i = V_{H_i}$ $1\leqq i\leqq r$ and for any $v\in V_i$, let $\psi_v^{(i)}$ denote the function $h \to \Phi(H_i;\partial(v):h)$ on $A_\mathfrak{p}(M)$ for M sufficiently large.

LEMMA 33. *Select nonzero elements* $v_i \in V_i$ $(1\leqq i\leqq r)$. *Then the functions* $\psi_{v_i}^{(i)}$ $1\leqq i\leqq r$ *are linearly independent over* C.

It is clear that for fixed $H' \in {}'\mathfrak{h}_\mathfrak{p}$, $\lambda\in L$ and $v \in S$,

$$\xi_\lambda(H';\partial(v):H)\exp\{-(-1)^{\frac{1}{2}}\langle H',H\rangle + \lambda(H)\}$$

is obviously a polynomial function of H. We denote by $p_\lambda^{(i)}$ this polynomial corresponding to $H' = H_i$ and $v = v_i$. Then if $H \in E(M)$,

$$\phi(H_i;\partial(v_i):H) = \sum_{\lambda\in L} p_\lambda^{(i)}(H)\exp\{(-1)^{\frac{1}{2}}\langle H_i,H\rangle - \lambda(H)\}.$$

Now suppose $c_1,\cdots,c_r$ are complex numbers such that

$$\sum_i c_i\phi(H_i;\partial(v_i):H) = 0 \qquad (H\in E(M)).$$

Then

$$\sum_{1\leqq i\leqq r}\sum_{\lambda\in L} c_ip_\lambda^{(i)}(H)\exp\{(-1)^{\frac{1}{2}}\langle H_i,H\rangle - \lambda(H)\} = 0$$

and it follows from Lemma 31, the corollary to Lemma 57 (§ 15) and our assumption that $(-1)^{\frac{1}{2}}(H_i - H_j)\notin L$ for $i\neq j$, that $c_ip_\lambda^{(i)} = 0$ for every i and every $\lambda\in L$. On the other hand it is obvious that $p_0^{(i)}(H) = v_i((-1)^{\frac{1}{2}}H)$ $(H\in\mathfrak{h}_\mathfrak{p})$. Therefore since $v_i\neq 0$, it follows that $p_0^{(i)}\neq 0$ and so $c_i = 0$. This proves the lemma.

It follows from the corollary to Lemma 32 that

$$\delta(q)\psi_v^{(i)} = \gamma(q:(-1)^{\frac{1}{2}}H_0)\psi_v^{(i)} \qquad (v\in V_i, q\in I_\mathfrak{g}, 1\leqq i\leqq r).$$

Moreover $\dim V_i = w'$ by Lemma 29. Hence if v_{ij} $1\leqq j\leqq w'$ is a base for V_i, we conclude from Lemma 33, that the w functions $\psi_{ij} = \psi_{v_{ij}}^{(i)}$ $(1\leqq i\leqq r,$

$1 \leqq j \leqq w'$) are linearly independent and $\delta(q)\psi_{ij} = \gamma(q:(-1)^{\frac{1}{2}}H_0)\psi_{ij}$ $(q \in I_\mathfrak{g})$. Therefore in view of Lemmas 18 and 23, we get the following result from the corollary of Theorem 2.

LEMMA 34. *Under the above assumptions there exist unique complex numbers* c_{ij} *such that*

$$e^{\rho(\log h)} \int_K \exp\{(-1)^{\frac{1}{2}}\langle H_0, H(hk)\rangle - \rho(H(hk))\} dk = \sum_{1 \leqq i \leqq r} \sum_{1 \leqq j \leqq w'} c_{ij}\psi_{ij}(h)$$

for all $h \in A_\mathfrak{p}(M)$.

In particular let us consider the case when $H_0 = 0$. Then $W' = W$ and $V = V_1$ is the set of all $v \in S(\mathfrak{h}_\mathfrak{p})$ such that $\langle v, p\rangle = 0$ for $p \in SJ_+$. Moreover since $\mathfrak{h}_{\mathfrak{p}_0} \subset {}'\mathfrak{h}_\mathfrak{p}$, all the required conditions for H_0 hold in this case. Therefore we obtain the following corollary.

COROLLARY. *There exists an element* $v \in V$ *and a number* $M \geqq 0$ *such that*

$$e^{\rho(\log h)} \int_K e^{-\rho(H(hk))} dk = \Phi(0; \partial(v):h)$$

for all $h \in A_\mathfrak{p}(M)$.

9. An important inequality. Define $\tilde{\theta}$ as in Section 5 and put $\| X \|^2 = -B(X, \tilde{\theta}(X))$ $(X \in \mathfrak{g})$. As before, we regard $\mathfrak{g}$ as a Hilbert space under the norm $\| X \|$. Let $\mathfrak{h}_{\mathfrak{p}_0}{}^+$ be the set of those points $H \in \mathfrak{h}_{\mathfrak{p}_0}$ where $\alpha(H) > 0$ for every $\alpha \in \Sigma$. We put $A_\mathfrak{p}{}^+ = \exp \mathfrak{h}_{\mathfrak{p}_0}{}^+$. Our main object in this section is to prove the following result which will play an important role later.

THEOREM 3. *There exists an integer* $d \geqq 0$ *and a positive number* a *such that*

$$\int_K e^{-\rho(H(hk))} dk \leqq a(1 + \| \log h \|)^d e^{-\rho(\log h)}$$

for all $h \in A_\mathfrak{p}{}^+$.

For the proof we need some auxiliary results. Let ${}^+\mathfrak{h}_{\mathfrak{p}_0}$ denote the set of all $H \in \mathfrak{h}_{\mathfrak{p}_0}$ such that $\langle H, H'\rangle \geqq 0$ for every H' in $\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Also let $\mathrm{Cl}(A_\mathfrak{p}{}^+)$ denote the closure of $A_\mathfrak{p}{}^+$ in $A_\mathfrak{p}$.

LEMMA 35. *Define* $\mathfrak{F}_0$ *as in Lemma 2. An element* $H' \in \mathfrak{h}_{\mathfrak{p}_0}$ *lies in* ${}^+\mathfrak{h}_{\mathfrak{p}_0}$ *if and only if* $\lambda(H') \geqq 0$ *for every* $\lambda \in \mathfrak{F}_0$. *Moreover* $\mathfrak{h}_{\mathfrak{p}_0}{}^+ \subset {}^+\mathfrak{h}_{\mathfrak{p}_0}$ *and* $\log h - H(hk) \in {}^+\mathfrak{h}_{\mathfrak{p}_0}$ *for* $h \in \mathrm{Cl}(A_\mathfrak{p}{}^+)$ *and* $k \in K$.

Select $\alpha_1, \cdots, \alpha_l \in \Sigma$ as in Section 3 and choose $H_i \in \mathfrak{h}_{\mathfrak{p}_0}$ such that[9] $\alpha_i(H_j) = \delta_{ij}$ $(1 \leqq i, j \leqq l)$. Then it is obvious that $\mathfrak{h}_{\mathfrak{p}_0}{}^+$ consists of all elements of the form $t_1H_1 + \cdots + t_lH_l$ where $t_1, \cdots, t_l$ are positive numbers. Therefore H' lies in ${}^+\mathfrak{h}_{\mathfrak{p}_0}$ if and only if $\langle H', H_i\rangle \geqq 0$ for every i. For any $\beta \in P$ define H_β as during the proof of Lemma 27 and, for a fixed i, consider the linear function μ_i on $\mathfrak{h}$ given by $\mu_i(H) = B(H_i, H)$ $(H \in \mathfrak{h})$. It is clear that $\mu_i(H_\beta) = \beta(H_i) \geqq 0$ for $\beta \in P$. Since $\beta(H_\beta)$ are positive rational numbers, we can choose a positive integer m such that $2m\mu_i(H_\beta)/\beta(H_\beta)$ is an integer for every $\beta \in P$ and every i $(1 \leqq i \leqq l)$. Let λ_i denote the restriction of $2m\mu_i$ on $\mathfrak{h}_{\mathfrak{p}}$. Then it follows from Theorem 1 of [5(b)] and Lemma 2 that $\lambda_i \in \mathfrak{F}_0$. Now suppose $H' \in \mathfrak{h}_{\mathfrak{p}_0}$. Then $\lambda_i(H') = 2m\langle H', H_i\rangle$ and $\langle \lambda_i, \alpha_j\rangle = 2m\alpha_j(H_i) = 2m\delta_{ji}$. Therefore if λ is any linear function on $\mathfrak{h}_{\mathfrak{p}}$, $\lambda = \sum_i c_i\lambda_i$ where $c_i = \langle\lambda, \alpha_i\rangle/2m$. But $\lambda \geqq s_{\alpha_i}\lambda$ if $\lambda \in \mathfrak{F}_0$ and so $2mc_i = \langle\lambda, \alpha_i\rangle \geqq 0$. Hence $\langle H', H_i\rangle \geqq 0$ $(1 \leqq i \leqq l)$ if and only if $\lambda(H') \geqq 0$ for every $\lambda \in \mathfrak{F}_0$. This proves the first statement of the lemma.

Now let π be an irreducible representation of $\mathfrak{g}$ on a finite-dimensional space V and let ϕ be a unit vector in V belonging to the highest weight Λ of π. Then (see [5(h), Lemma 2]) every other weight of π is of the form $\Lambda - (m_1\beta_1 + \cdots + m_r\beta_r)$ where $\beta_1, \cdots, \beta_r \in P$ and $m_1, \cdots, m_r$ are positive integers. Hence if $H \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$, it follows that $\Lambda(H) \geqq \Lambda'(H)$ for every weight Λ' of π. But since $\pi(H)$ is a self-adjoint operator of trace zero, this implies that $\Lambda(H) \geqq 0$. Similarly if $h \in \mathrm{Cl}(A_{\mathfrak{p}}{}^+)$, $e^{\Lambda(\log h)}$ is the largest eigenvalue of the self-adjoint operator $\pi(h)$. Therefore

$$|\pi(hk)\phi| \leqq e^{\Lambda(\log h)}\,|\pi(k)\phi| = e^{\Lambda(\log h)}$$

for $k \in K$. However it is obvious that $|\pi(hk)\phi| = e^{\Lambda(H(hk))}$ and so $\Lambda(\log h - H(hk)) \geqq 0$. This shows in particular that $\lambda(H) \geqq 0$ and $\lambda(\log h - H(hk)) \geqq 0$ for $\lambda \in \mathfrak{F}_0$. Therefore by the criterion established above, H and $\log h - H(hk)$ lie in ${}^+\mathfrak{h}_{\mathfrak{p}_0}$. Thus the lemma is proved.

COROLLARY 1. *Let H and H' be two elements in $\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Then $\langle H', H\rangle > \langle H', sH\rangle$ for $s \neq 1$ in W.*

Fix an element $s \neq 1$ in W and select $k \in K$ such that $\mathrm{Ad}(k)H = sH$. Then $\pi(sH) = \pi(k)\pi(H)\pi(k^{-1})$ in the above notation. Therefore since $\Lambda(H)$ is the greatest eigenvalue of $\pi(H)$, it follows that $\Lambda(sH) \leqq \Lambda(H)$. But in view of Lemma 35, this implies that $H - sH \in {}^+\mathfrak{h}_{\mathfrak{p}_0}$. Now $\lambda_1, \cdots, \lambda_l$ are linearly independent and by Lemma 6 $H \neq sH$ since $H \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$. Therefore $\lambda_i(H - sH) \neq 0$ for some i. Moreover we have seen that if λ is any linear function on $\mathfrak{h}_{\mathfrak{p}}$, $\lambda = \sum_i c_i\lambda_i$ where $c_i = \langle\lambda, \alpha_i\rangle/2m$. Therefore $\langle H', H - sH\rangle$

$=(2m)^{-1}\sum_{1\leqq i\leqq l}\alpha_i(H')\lambda_i(H-sH)$. But from Lemma 35, $\lambda_i(H-sH)$ are non-negative and $\alpha_i(H')>0$ $(1\leqq i\leqq l)$ since $H'\in\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Therefore $\langle H',H-sH\rangle>0$.

From [5(j), Lemma 37] we can choose $s_0\in W$ such that $s_0\mathfrak{h}_{\mathfrak{p}_0}{}^+=-\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Put $H^*=-s_0H$ for any $H\in\mathfrak{h}_{\mathfrak{p}}$. It is obvious that the mapping $\alpha\to-s_0\alpha$ $(\alpha\in\Sigma)$ is a permutation on Σ and therefore $\rho(H^*)=\rho(H)$.

COROLLARY 2. *$(\log h)^*+H(hk)\in{}^+\mathfrak{h}_{\mathfrak{p}_0}$ for $h\in\mathrm{Cl}(A_{\mathfrak{p}}{}^+)$ and $k\in K$.*

Fix h and k and let $hk=k'\exp H(hk)n$ $(k'\in K, n\in N)$. Then $H(hk)=-H(h^{-1}k')$ (see [5(c), Lemma 36]). Now select $k_0\in K$ such that $\mathrm{Ad}(k_0)H'=s_0H'$ for every H' in $\mathfrak{h}_{\mathfrak{p}_0}$. Then if $h^*=\exp(\log h)^*$, it is obvious that $h^*=k_0h^{-1}k_0{}^{-1}$ and therefore $H(h^*k_0k')=H(h^{-1}k')=-H(hk)$. But from Lemma 35, this implies that

$$\log h^*+H(hk)=\log h^*-H(h^*k_0k')\in{}^+\mathfrak{h}_{\mathfrak{p}_0}.$$

COROLLARY 3. *$\rho(\log h)\geqq|\rho(H(hk))|$ for $h\in\mathrm{Cl}(A_{\mathfrak{p}}{}^+)$ and $k\in K$.*

It follows from the definition of ρ that $s_\alpha\rho<\rho$ and therefore $\langle\rho,\alpha\rangle>0$ for any $\alpha\in\Sigma$. Hence $H_\rho\in\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Moreover $\rho(\log h^*)=\rho(\log h)$ as we have seen above. Hence our assertion follows from the fact that $\log h-H(hk)$ and $\log h^*+H(hk)$ are both in ${}^+\mathfrak{h}_{\mathfrak{p}_0}$.

Now put $\psi(h)=e^{\rho(\log h)}\int_K e^{-\rho(H(hk))}dk$ $(h\in A_{\mathfrak{p}})$.

LEMMA 36. *$\psi(h)\leqq\psi(hh_1)$ for $h\in A_{\mathfrak{p}}$ and $h_1\in\mathrm{Cl}(A_{\mathfrak{p}}{}^+)$.*

Fix h and h_1 and for any $k\in K$, let k' denote the unique element in K such that $h_1k\in k'A_{\mathfrak{p}}N$. Then $k\to k'$ is a homeomorphism of K, $H(hh_1k)=H(hk')+H(h_1k)$ and $dk'=e^{-2\rho(H(h_1k))}dk$ (see [5(c), pp. 240-241]). Hence

$$\int_K e^{-\rho(H(hk))}dk=\int_K e^{-\rho(H(hk'))}dk'=\int_K\exp\{-\rho(H(hk'))-2\rho(H(h_1k))\}dk$$
$$=\int_K\exp\{-\rho(H(hh_1k))-\rho(H(h_1k))\}dk\leqq e^{\rho(\log h_1)}\int_K e^{-\rho(H(hh_1k))}dk$$

from Corollary 3 to Lemma 35. This implies that $\psi(h)\leqq\psi(hh_1)$.

Now we come to the proof of Theorem 3. Select $H_0\in\mathfrak{h}_{\mathfrak{p}_0}{}^+$ such that $\alpha_i(H_0)=1$ $(1\leqq i\leqq l)$ and put $F(t)=\psi(\exp tH_0)$ $(t\in R)$. Then in the notation of Section 8, $F(t)=\phi(0;\partial(v):tH_0)$ for $t>M$, where v and M are defined as in the corollary to Lemma 34. Let d be the degree of v. Then it follows from Lemma 31 that

$$F(t)=\sum_{\lambda\in L}p_\lambda(t)e^{-t\lambda(H_0)}\qquad(t>M),$$

where p_λ are polynomials of degree $\leqq d$ and the series $\sum_{\lambda \in L} | p_\lambda(t) e^{-t\lambda(H_0)} |$ converges uniformly for $t > M$ (if M is chosen sufficiently large). Hence we can find a finite number of distinct elements $\lambda_0 = 0, \lambda_1, \cdots \lambda_r \in L$ such that

$$| F(t) - \sum_{0 \leqq i \leqq r} p_{\lambda_i}(t) e^{-t\lambda_i(H_0)} | \leqq 1$$

for $t > M$. But since $\lambda(H_0) = m(\lambda)$ (in the notation of Lemma 28), it is obvious that

$$\operatorname*{Lim}_{t \to +\infty} \sum_{1 \leqq i \leqq r} p_{\lambda_i}(t) e^{-t\lambda_i(H_0)} = 0.$$

Therefore $F(t) \leqq 2 + p_0(t)$ for all sufficiently large positive values of t. Since the degree of p_0 is $\leqq d$, this means that we can select a positive constant a such that $F(t) \leqq a(1 + t)^d$ for all $t \geqq 0$.

Let $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$ denote the closure of $\mathfrak{h}_{\mathfrak{p}_0}{}^+$ in $\mathfrak{h}_{\mathfrak{p}_0}$ and put $\beta(H) = \max_{1 \leqq i \leqq l} \alpha_i(H)$ for $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Then it is obvious that $\beta(H)H_0 - H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. Hence it follows from Lemma 36 that $\psi(\exp H) \leqq F(\beta(H)) \leqq a(1 + \beta(H))^d$ for $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. On the other hand $\| H \|^2 = \mathrm{sp}(\mathrm{ad}\, H)^2 \geqq \sum_{1 \leqq i \leqq l} \alpha_i(H)^2 \geqq \beta(H)^2$. Therefore

$$\psi(\exp H) \leqq a(1 + \| H \|)^d$$

and this proves the theorem.

Remark. Let d_π denote the degree of the polynomial function π of Section 3 and define V as in the corollary to Lemma 34. Then it follows from Lemma 16 that no nonzero element in V can have a degree greater than d_π. This shows that $d \leqq d_\pi$.

10. The function *c*. For any $\lambda \in L'$ define σ_λ (as in Section 8) to be the hyperplane consisting of those points $H \in \mathfrak{h}_{\mathfrak{p}}$ where $\langle \lambda, \lambda \rangle = 2(-1)^{\frac{1}{2}}\lambda(H)$ and let $\tau_\lambda(s, t)$ $(s, t \in W)$ denote the set of all $H \in \mathfrak{h}_{\mathfrak{p}}$ for which $(-1)^{\frac{1}{2}}(sH - tH) = H_\lambda$. Then if $\mathfrak{S}$ is the collection of all hyperplanes of the form $s\sigma_\lambda$ or $\tau_\lambda(s, t)$ $(s, t \in W; \lambda \in L')$, it is obvious that any compact subset of $\mathfrak{h}_{\mathfrak{p}}$ meets only a finite number of hyperplanes in $\mathfrak{S}$. Let ${}^*\mathfrak{h}_{\mathfrak{p}}$ be the complement (in $\mathfrak{h}_{\mathfrak{p}}$) of the union of all hyperplanes in $\mathfrak{S}$. Then ${}^*\mathfrak{h}_{\mathfrak{p}}$ is an open, connected and dense subset of $\mathfrak{h}_{\mathfrak{p}}$. Moreover it follows from its definition that ${}^*\mathfrak{h}_{\mathfrak{p}}$ is invariant under W. Define π as in Lemma 11 and let ${}^*\mathfrak{h}_{\mathfrak{p}}{}'$ be the set of those $H \in {}^*\mathfrak{h}_{\mathfrak{p}}$ where $\pi(H) \neq 0$. Since the zeros of π consist of a finite number of hyperplanes, ${}^*\mathfrak{h}_{\mathfrak{p}}{}'$ is also connected. We shall now use the notation of Section 8.

LEMMA 37. *There exists a holomorphic function* $\boldsymbol{c}$ *on* ${}^*\mathfrak{h}_{\mathfrak{p}}{}'$ *with the* *following property. For any compact subset U of ${}^*\mathfrak{h}_{\mathfrak{p}}$, we can select a number $M \geqq 0$ such that*

$$e^{\rho(\log h)}\int_K \exp\{(-1)^{\frac{1}{2}}\langle H_0, H(hk)\rangle - \rho(H(hk))\}dk$$
$$= \sum_{s\in W} \boldsymbol{c}(sH_0)\Phi(sH_0:h)$$

for $H_0 \in U \cap {}^*\mathfrak{h}_{\mathfrak{p}}'$ and $h \in A_{\mathfrak{p}}(M)$. (Here Φ has the same meaning as in Lemma 30.)

Put

$$\psi(H_0:h) = e^{\rho(\log h)}\int_K \exp\{(-1)^{\frac{1}{2}}\langle H_0, H(hk)\rangle - \rho(H(hk))\}dk$$

for $H_0 \in \mathfrak{h}_{\mathfrak{p}}$ and $h \in A_{\mathfrak{p}}$. It is obvious that for fixed $h \in A_{\mathfrak{p}}$ and[22] $u \in \mathfrak{H}_{\mathfrak{p}}$, $\psi(H_0:h;u)$ is a holomorphic function of H_0. Moreover if $H_0 \in {}^*\mathfrak{h}_{\mathfrak{p}}'$, the w elements sH_0 $(s \in W)$ are all distinct. Therefore it follows from Lemma 34 that there exist unique complex numbers $\boldsymbol{c}_s(H_0)$ such that

$$\psi(H_0:h) = \sum_{s\in W} \boldsymbol{c}_s(H_0)\Phi(sH_0:h)$$

for $h \in A_{\mathfrak{p}}(M)$ provided M is sufficiently large. In view of Corollary 1 of Lemma 28, it is sufficient to show that $\boldsymbol{c}_s$ $(s \in W)$, regarded as functions of H_0, are holomorphic on ${}^*\mathfrak{h}_{\mathfrak{p}}'$ and $\boldsymbol{c}_s(H_0) = \boldsymbol{c}_1(sH_0)$ $(H_0 \in {}^*\mathfrak{h}_{\mathfrak{p}}')$.

Let U_0 be a nonempty open set in ${}^*\mathfrak{h}_{\mathfrak{p}}$ which is invariant under W. We assume that the closure of U_0 in ${}^*\mathfrak{h}_{\mathfrak{p}}$ is compact. Select M so large that for any $H \in U_0, \Phi(H:h)$ is defined for $h \in A_{\mathfrak{p}}(M)$ and choose $u_1, \cdots, u_w \in \mathfrak{H}_{\mathfrak{p}}$ as in the corollary to Lemma 8. Also put $U_0' = U_0 \cap {}^*\mathfrak{h}_{\mathfrak{p}}'$.

LEMMA 38. *Let $s_1, s_2, \cdots, s_w$ be all the elements of W. Then* $\det\{\Phi(s_iH_0:h_0;u_j)\}_{1\leqq i,j\leqq w} \neq 0$ *for any $H_0 \in U_0'$ and $h_0 \in A_{\mathfrak{p}}(M)$.*

For otherwise we can select complex numbers a_s $(s \in W)$, not all zero, such that $\sum_{s\in W} a_s\Phi(sH_0:h_0;u_j) = 0$ $(1 \leqq j \leqq w)$. Put $f(h) = \sum_{s\in W} a_s\Phi(sH_0:h)$ for $h \in A_{\mathfrak{p}}(M)$. Then f is an analytic function on $A_{\mathfrak{p}}(M)$ and it follows from Lemma 30 that $\delta(q)f = \gamma(q:(-1)^{\frac{1}{2}}H_0)f$ for $q \in I_{\mathfrak{g}}$. Therefore since $f(h_0;u_j) = 0$ $(1 \leqq j \leqq w)$, we conclude from Theorem 2 that $f(h_0;u) = 0$ for every $u \in \mathfrak{H}_{\mathfrak{p}}$. But since f is analytic and $A_{\mathfrak{p}}(M)$ is connected, this implies that $f = 0$. However this contradicts Lemma 33 since $W' = \{1\}$ in the present case.

Now in order to complete the proof of Lemma 37, fix $h_0 \in A_{\mathfrak{p}}(M)$. Then by Lemma 38 there exist holomorphic functions a_{si} on U_0' $(s \in W$, $1 \leqq i \leqq w)$ such that $\sum_{1\leqq i\leqq w} a_{si}(H)\Phi(s'H:h_0;u_i) = 1$ or 0 according as $s = s'$

or not $(s, s' \in W, H \in U_0')$. Therefore $\boldsymbol{c}_s(H) = \sum_{1 \leqq i \leqq w} a_{si}(H)\psi(H : h_0 ; u_i)$ $(s \in W, H \in U_0')$ and this proves that $\boldsymbol{c}_s$ is holomorphic on U_0'. On the other hand we know from the corollary to Lemma 17 that $\psi(sH : h_0) = \psi(H : h_0)$ for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}}$. This implies that $\boldsymbol{c}_s(H) = \boldsymbol{c}(sH)$ $(s \in W, H \in U_0)$ where $\boldsymbol{c} = \boldsymbol{c}_1$. Hence Lemma 37 is now proved completely.

11. A formula for *c*. We shall now derive an explicit formula for $\boldsymbol{c}$ which will be valid on a suitable subdomain of ${}^*\mathfrak{h}_{\mathfrak{p}}'$. For any root $\alpha \in P$, define X_α and $X_{-\alpha}$ as in Section 7 and put $\mathfrak{n}^+ = \sum_{\alpha \in P} CX_\alpha$, $\mathfrak{n}^- = \sum_{\alpha \in P} CX_{-\alpha}$. Let N_c^+, N_c^- and A_c denote the complex-analytic subgroups of G_c corresponding to $\mathfrak{n}^+$, $\mathfrak{n}^-$ and $\mathfrak{h}$ respectively and put $G_c' = N_c^- A_c N_c^+$. Since $\mathfrak{g}$ is the direct sum of $\mathfrak{n}^-$, $\mathfrak{h}$ and $\mathfrak{n}^+$, it follows easily that G_c' is open in G_c. We regard G_c' as an open submanifold of G_c. Then (see [5(i), Lemma 1]) the mapping $(n_1, a, n_2) \rightarrow n_1 a n_2$ $(n_1 \in N_c^-, a \in A_c, n_2 \in N_c^+)$ is a one-one holomorphic mapping of $N_c^- \times A_c \times N_c^+$ onto G_c' which is regular everywhere. For any $z \in G_c'$, let $a(z)$ denote the unique element in A_c such that $z \in N_c^- a(z) N_c^+$. Then $z \rightarrow a(z)$ is a holomorphic mapping of G_c' onto A_c.

LEMMA 39. *Let n_r', a_r, n_r $(r \geqq 1)$ be three sequences in N_c^-, A_c and N_c^+ respectively such that a_r and $n_r' a_r n_r$ converge in G_c. Then n_r' and n_r are also convergent.*

Obviously it would be enough to prove that n_r' is convergent. Since A_c is closed in G_c, a_r converges to an element $a_0 \in A_c$. Let π be an irreducible representation of $\mathfrak{g}$ (and therefore also of G_c) on a finite-dimensional vector space V and ξ a unit vector belonging to the highest weight Λ of π. For any root α define H_α as in Section 7. Then by choosing π suitably, we can assume (see [5(b), Theorem 1]) that $\Lambda(H_\alpha) > 0$ for every $\alpha \in P$. Let χ denote the character of A_c such that $\pi(a)\xi = \chi(a)\xi$ for $a \in A_c$. Then if $n_r' a_r n_r$ converges to z in G_c, it is clear that

$$\pi(n_r')\xi = \chi(a_r^{-1})\pi(n_r' a_r n_r)\xi \rightarrow \chi(a_0^{-1})\pi(z)\xi.$$

Since $\mathfrak{n}^-$ is a nilpotent Lie algebra, we can select $Y_r \in \mathfrak{n}^-$ such that $\exp Y_r = n_r'$. Then it would be sufficient to prove that Y_r converges in $\mathfrak{n}^-$. Thus it remains to prove the following result.

LEMMA 40. *Suppose Y varies in $\mathfrak{n}^-$ in such a way that $\pi(\exp Y)\xi$ converges in V. Then Y itself converges in $\mathfrak{n}^-$.*

Let $\beta_1 < \beta_2 < \cdots < \beta_r$ be all the roots in P. Then $Y = \sum_{1 \leqq i \leqq r} t_i(Y) X_{-\beta_i}$

$(t_i(Y) \in C)$ and it would be sufficient to prove that $t_i(Y)$ converges in C for every i. Hence suppose that this is false and let j be the least index such that $t_j(Y)$ does not converge. Let V_j be the subspace of V consisting of all vectors belonging to the weight $\Lambda - \beta_j$ and let E_j denote the orthogonal projection of V on V_j. Then

$$E_j\pi(\exp Y)\xi = \sum_{m \geqq 0} E_j\pi(Y^m)\xi/m!.$$

But if $Y' = \sum_{1 \leqq i < j} t_i(Y)X_{-\beta_i}$, it is obvious that $E_j\pi(Y^m)\xi = E_j\pi(Y'^m)\xi$ for $m > 1$. Moreover $E_j\pi(Y')\xi = 0$ while $E_j\pi(Y)\xi = t_j(Y)\pi(X_{-\beta_j})\xi$. Hence

$$E_j\pi(\exp Y)\xi = t_j(Y)\pi(X_{-\beta_j})\xi + E_j\pi(\exp Y')\xi.$$

On the other hand, in view of our hypothesis and the definition of j, both $\pi(\exp Y)\xi$ and $\pi(\exp Y')\xi$ converge in V. Therefore the same holds for $t_j(Y)\pi(X_{-\beta_j})\xi$. But $\pi(X_{-\beta_j})\xi \neq 0$ since $\Lambda(H_{\beta_j}) > 0$ (see [5(h), Lemma 1]). Hence $t_j(Y)$ also converges in C. As this contradicts the definition of j, our assertion follows.

COROLLARY 1. *Let z be an element in G_c. Then $z \in G_c'$ if and only if* $(\xi, \pi(z)\xi) \neq 0$.

Put $f(z) = (\xi, \pi(z)\xi)$ and let G_c'' be the set of all $z \in G_c$ where $f(z) \neq 0$. Since f is a holomorphic function on G_c and $f(1) = 1$, its set of zeros is a complex subvariety of G_c of one complex dimension less. Therefore G_c'' is an open connected subset of G_c. Moreover if $z \in G_c'$, it is obvious that $f(z) = \chi(a(z)) \neq 0$. Therefore $G_c' \subset G_c''$. Hence it would be sufficient to show that G_c' is closed in G_c''. Let z_r $(r \geqq 1)$ be a sequence in G_c' which converges to $z \in G_c''$. Suppose $z_r = n_r'a_rn_r$ $(n_r' \in N_c^-, a_r \in A_c, n_r \in N_c^+)$. Then $\chi(a_r) = f(z_r) \rightarrow f(z) \neq 0$ and therefore $\pi(n_r')\xi = \chi(a_r^{-1})\pi(z_r)\xi \rightarrow f(z)^{-1}\pi(z)\xi$. But then by the above lemma, n_r' converges to an element n' in N_c^-. However this implies that $a_rn_r = n_r'^{-1}z_r \rightarrow n'^{-1}z$. On the other hand $A_cN_c^+$ is closed in G_c and hence $n'^{-1}z \in A_cN_c^+$. This proves that $z \in G_c'$ and therefore G_c' is closed in G_c''.

COROLLARY 2. *Put $K' = K \cap G_c'$. Then K' is an open dense subset of K whose complement (in K) is of measure zero with respect to the Haar measure of K.*

Let g be the restriction on K of the function f defined above. Then g is an analytic function which is not identically zero since $g(1) = 1$. Moreover K' is the set of all points $k \in K$ where $g(k) \neq 0$. From this our statement follows immediately.

Since G_c is simply connected, we can extend θ to an automorphism of G_c. Put $\mathfrak{n} = \sum_{\alpha \in P_+} CX_\alpha$ and $\bar{\mathfrak{n}} = \theta(\mathfrak{n}) = \sum_{\alpha \in P_+} CX_{-\alpha}$ and let N_c, $\bar{N}_c$ denote the complex analytic subgroups of G_c corresponding to $\mathfrak{n}$, $\bar{\mathfrak{n}}$ respectively. Also let Ξ_c and $\mathfrak{z}$ denote the centralizers of $\mathfrak{h}_{\mathfrak{p}}$ in G_c and $\mathfrak{g}$ respectively. Since $\mathfrak{n}^+ + \mathfrak{h}_{\mathfrak{p}} \subset \mathfrak{n} + \mathfrak{z}$, it follows easily that $\bar{N}_c \Xi_c N_c \supset N_c^- A_c N_c^+ = G_c'$.

LEMMA 41. *Suppose* $Y \in \bar{\mathfrak{n}}$ *and* $\exp(\operatorname{ad} Y)$ *maps* $\mathfrak{n}$ *into itself. Then* $Y = 0$.

Otherwise suppose that $Y \neq 0$. Let $\beta_1 < \beta_2 < \cdots < \beta_r$ be all the roots in P_+. Then $Y = \sum_i c_i X_{-\beta_i}$ where $c_i \in C$. Let k be the least integer such that $c_k \neq 0$. Then it is obvious that $\exp(\operatorname{ad} Y) X_{\beta_k} - X_{\beta_k} \equiv -c_k H_{\beta_k} \bmod \mathfrak{n}^-$. Therefore since the sum $\mathfrak{h} + \mathfrak{n}^+ + \mathfrak{n}^-$ is direct, it follows that $\exp(\operatorname{ad} Y) X_{\beta_k}$ does not lie in $\mathfrak{n}^+ + \mathfrak{n}^-$. But this contradicts our hypothesis that $\exp(\operatorname{ad} Y)$ maps $\mathfrak{n}$ into itself. Hence the lemma.

COROLLARY. $\bar{N}_c \cap (\Xi_c N_c) = \{1\}$ *and* $\Xi_c \cap N_c = \{1\}$.

Suppose $y \in \bar{N}_c \cap (\Xi_c N_c)$. Then $y = \exp Y$ for some $Y \in \bar{\mathfrak{n}}$ and $\operatorname{Ad}(y)$ leaves $\mathfrak{n}$ invariant. Hence $Y = 0$ and so $y = 1$. Now suppose $x \in \Xi_c \cap N_c$. Then $x = \exp X$ for some $X \in \mathfrak{n}$. Put $Y = \theta(X)$. Since $x \in \Xi_c$, $\operatorname{Ad}(x)$ leaves $\bar{\mathfrak{n}}$ invariant and therefore $\exp(\operatorname{ad} Y)$ leaves $\mathfrak{n}$ invariant. Hence $Y = 0$. This proves that $x = 1$.

Define N as in Section 2 and let M be the centralizer of $A_{\mathfrak{p}}$ in K. Put $S = MA_{\mathfrak{p}}N$. Obviously S is a subgroup of G.

LEMMA 42. $G \cap (\bar{N}_c \Xi_c N_c) = \bar{N} S$ *where* $\bar{N} = \theta(N)$.

Suppose $x \in G \cap (\bar{N}_c \Xi_c N_c)$. Then $x = \bar{n} \xi n$ $(\bar{n} \in \bar{N}_c, \xi \in \Xi_c, n \in N_c)$. Let η denote the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{g}_0$. We extend it to a real automorphism of G_c. Then $x = \eta(x) = \eta(\bar{n})\eta(\xi)\eta(n)$. Since η maps $\mathfrak{n}$ and $\bar{\mathfrak{n}}$ into themselves, it follows from the corollary to Lemma 41 that $\eta(\bar{n}) = \bar{n}$ and $\eta(n) = n$. Choose $X \in \mathfrak{n}$ and $Y \in \bar{\mathfrak{n}}$ such that $\exp X = n$, $\exp Y = \bar{n}$. Since the exponential mapping is univalent on both $\mathfrak{n}$ and $\bar{\mathfrak{n}}$, we conclude that X and Y are left fixed by η. Hence $X \in \mathfrak{n} \cap \mathfrak{g}_0$, $Y \in \bar{\mathfrak{n}} \cap \mathfrak{g}_0$ and therefore $n \in N$, $\bar{n} \in \bar{N}$ and $\xi \in G \cap \Xi_c$. This shows that $G \cap (\bar{N}_c \Xi_c N_c) = \bar{N}(G \cap \Xi_c)N$. But since $MA_{\mathfrak{p}}$ is the centralizer[13] of $A_{\mathfrak{p}}$ in G, it follows that $G \cap \Xi_c = MA_{\mathfrak{p}}$ and therefore $G \cap (\bar{N}_c \Xi_c N_c) = \bar{N} S$.

COROLLARY. *Put* $K_1 = K \cap (\bar{N} S)$. *Then* $K_1 \supset K'$.

We have seen above that $\bar{N}_c \Xi_c N_c \supset G_c'$ and therefore $K_1 = K \cap (\bar{N}_c \Xi_c N_c) \supset K \cap G_c' = K'$.

LEMMA 43. *Let* $\bar{n} \in \bar{N}$ *and* $h \in \mathrm{Cl}(A_{\mathfrak{p}}^{+})$. *Then both* $H(\bar{n})$ and $H(\bar{n}) - H(h\bar{n}h^{-1})$ *lie in* ${}^{+}\mathfrak{h}_{\mathfrak{p}_0}$.

Let π be an irreducible representation of $\mathfrak{g}$ on a finite-dimensional space and let ϕ be a unit vector belonging to the highest weight Λ of π. Then $|\pi(\bar{n})\phi| \geqq e^{\Lambda(H(\bar{n}))}$. Moreover since $h \in \mathrm{Cl}(A_{\mathfrak{p}}^{+})$, $e^{\Lambda(\log h)}$ is the greatest eigenvalue of the self-adjoint operator $\pi(h)$ (see the proof of Lemma 35). Hence

$$e^{\Lambda(H(h\bar{n}h^{-1}))} = |\pi(h\bar{n}h^{-1})\phi| \leqq e^{\Lambda(\log h)} |\pi(\bar{n}h^{-1})\phi| = |\pi(\bar{n})\phi| = e^{\Lambda(H(\bar{n}))}.$$

This proves that $\Lambda(H(\bar{n})) - \Lambda(H(h\bar{n}h^{-1})) \geqq 0$. Now choose $Y \in \bar{\mathfrak{n}}$ such that $\bar{n} = \exp Y$. Then $\pi(\exp Y)\phi - \phi$ is obviously a sum of vectors belonging to weights lower than Λ. Hence ϕ and $\pi(\bar{n})\phi - \phi$ are mutually orthogonal and therefore $|\pi(\bar{n})\phi|^2 = |\phi|^2 + |\pi(\bar{n})\phi - \phi|^2 \geqq 1$. This shows that $\Lambda(H(\bar{n})) \geqq 0$ and the required statements now follow from Lemma 35.

COROLLARY. $\rho(H(\bar{n})) \geqq 0$ *for* $\bar{n} \in \bar{N}$.

Since $H_\rho \in \mathfrak{h}_{\mathfrak{p}_0}{}^{+}$, this is an immediate consequence of the above lemma.

For any $\bar{n} \in \bar{N}$, let $k(\bar{n})$ denote the unique element in K such that $\bar{n} \in k(\bar{n})A_{\mathfrak{p}}N$. We denote by $C(K)$ the space of continuous functions on K and by dm the normalized Haar measure on M.

LEMMA 44. *The Haar measure* $d\bar{n}$ *on* $\bar{N}$ *can be so normalized that*

$$\int_K f(k)\,dk = \int_{M \times \bar{N}} f(mk(\bar{n}))\,e^{-2\rho(H(\bar{n}))}\,dm\,d\bar{n}$$

for any $f \in C(K)$. *This normalization is characterized by the condition that*

$$\int_{\bar{N}} e^{-2\rho(H(\bar{n}))}\,d\bar{n} = 1.$$

Put $S_0 = A_{\mathfrak{p}}N$ and let ds_0 denote the left-invariant measure on S_0. Similarly let ds denote the left-invariant measure on $S = MS_0$. We may assume that $ds = dm\,ds_0$ $(s = ms_0, m \in M, s_0 \in S_0)$. Let dx denote the Haar measure on G and $D(s)$ $(s \in S)$ the absolute value of the determinant of the restriction of $\mathrm{Ad}(s)$ on $\mathfrak{z} + \mathfrak{n}$. Since $G = KS_0$, a simple calculation (see [5(c), Lemma 35]) shows that

$$\int_G F(x)\,dx = \int_{K \times S_0} F(ks_0)D(s_0)\,dk\,ds_0 \qquad (F \in C_c(G)),^{17}$$

provided dx is suitably normalized. Now $\bar{N}S = K_1S_0$ and therefore we conclude from Corollary 2 to Lemma 40 and the corollary to Lemma 42 that the complement of $\bar{N}S$ in G is of measure zero. On the other hand the mapping $(\bar{n}, s) \to \bar{n}s$ of $\bar{N} \times S$ into G is univalent from the corollary to Lemma 41. Put $\mathfrak{n}_0 = \mathfrak{n} \cap \mathfrak{g}_0$ and $\mathfrak{z}_0 = \mathfrak{z} \cap \mathfrak{g}_0$. Then $\mathfrak{g}_0 = \theta(\mathfrak{n}_0) + \mathfrak{z}_0$ and from this it follows easily that the above mapping is everywhere regular. Moreover a straightforward calculation shows that $dx = D(s)\,d\bar{n}ds$ $(x = \bar{n}s)$. Therefore

$$\int_{K\times S_0} F(ks_0)D(s_0)\,dkds_0 = \int_{\bar{N}\times S} F(\bar{n}s)D(s)\,d\bar{n}ds.$$

Now $\bar{n} = k(\bar{n})s(\bar{n})$ where $s(\bar{n}) \in S_0$. Therefore it follows from the left-invariance of ds that

$$\int_{\bar{N}\times S} F(\bar{n}s)D(s)\,d\bar{n}ds = \int_{\bar{N}\times S} F(k(\bar{n})s)D(s)D(s(\bar{n}))^{-1}\,d\bar{n}ds.$$

But $D(s(\bar{n})) = e^{2\rho(H(\bar{n}))}$. Hence

$$\int_{K\times S_0} F(ks_0)D(s_0)\,dkds_0 = \int F(k(\bar{n})ms_0)D(s_0)e^{-2\rho(H(\bar{n}))}dmd\bar{n}ds_0$$

because $D(m) = 1$. Now select a function[17] $g \in C_c(S_0)$ such that

$$\int g(s_0)D(s_0)\,ds_0 = 1$$

and define F by $F(ks_0) = f(k)g(s_0)$ $(k \in K, s_0 \in S_0)$ where f is a given function in $C(K)$. Then

$$\int F(ks_0)D(s_0)\,dkds_0 = \int_K f(k)\,dk$$

while

$$\int F(k(\bar{n})ms_0)D(s_0)e^{-2\rho(H(\bar{n}))}dmd\bar{n}ds_0 = \int f(k(\bar{n})m)e^{-2\rho(H(\bar{n}))}d\bar{n}dm.$$

But for a fixed $m \in M$, the measure $d\bar{n}$ is invariant under the transformation $\bar{n} \to \bar{n}' = m^{-1}\bar{n}m$ and $k(\bar{n}') = m^{-1}k(\bar{n})m$, $H(\bar{n}') = H(\bar{n})$. Therefore

$$\int_K f(k)\,dk = \int f(mk(\bar{n}))e^{-2\rho(H(\bar{n}))}dmd\bar{n}.$$

In particular if we take $f = 1$, we get the relation $\int e^{-2\rho(H(\bar{n}))}d\bar{n} = 1$.

COROLLARY 1. *Let* ν *be a linear function on* $\mathfrak{h}_{\mathfrak{p}}$ *and put* $\nu_+ = \nu + \rho$, $\nu_- = \nu - \rho$. *Then*

$$\int_K \exp\{\nu(H(hk)) - \rho(H(hk))\}dk$$
$$= e^{\nu_-(\log h)}\int_{\bar{N}} \exp\{\nu_-(H(h\bar{n}h^{-1})) - \nu_+(H(\bar{n}))\}d\bar{n}$$

for $h \in A_{\mathfrak{p}}$.

Let $\psi(h)$ denote the left side. Then it follows from the above lemma that

$$\psi(h) = \int \exp\{\nu_-(H(hmk(\bar n)) - 2\rho(H(\bar n))\} dm d\bar n.$$

But m commutes with h and therefore $H(hmk(\bar n)) = H(hk(\bar n))$. Also $\bar n \in k(\bar n) \exp H(\bar n) N$ and therefore $h\bar n \exp(-H(\bar n)) \in hk(\bar n)N$. But this implies that $H(hk(\bar n)) = H(h\bar n) - H(\bar n) = \log h + H(h\bar n h^{-1}) - H(\bar n)$. Therefore

$$\psi(h) = e^{\nu_-(\log h)} \int \exp\{\nu_-(H(h\bar n h^{-1})) - \nu_+(H(\bar n))\} d\bar n.$$

COROLLARY 2.

$$e^{\rho(\log h)} \int_K e^{-\rho(H(hk))} dk = \int_{\bar N} \exp\{-\rho(H(h\bar n h^{-1})) - \rho(H(\bar n))\} d\bar n$$

for $h \in A_{\mathfrak{p}}$.

This follows by putting $\nu = 0$ in Corollary 1.

The following lemma is of decisive significance for our purpose.

LEMMA 45. *Let* ϵ *be a positive number and* d *the integer of Theorem* 3. *Then*

$$\int_{\bar N} e^{-\rho(H(\bar n))} \{1 + \rho(H(\bar n))\}^{-d-\epsilon} d\bar n < \infty.$$

Select an element $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$ and put $h_t = \exp tH_0$ $(t \in R)$. Then it follows from Theorem 3 and Corollary 2 above that

$$\int_{\bar N} \exp\{-\rho(H(h_t \bar n h_t^{-1})) - \rho(H(\bar n))\} d\bar n \leqq c(1+t)^d \qquad (t \geqq 0)$$

for a suitable positive number c. Put $\Lambda = \frac{1}{2} \sum_{\alpha \in P} \alpha$ and let σ denote the irreducible finite-dimensional representation of $\mathfrak{g}$ on a space V with the highest weight[28] Λ. Choose a unit vector ϕ_0 in V belonging to the weight Λ. Then

$$|\sigma(h\bar n h^{-1})\phi_0|^2 = \exp 2\rho(H(h\bar n h^{-1}))$$

for $h \in A_{\mathfrak{p}}$ and $\bar n \in \bar N$. Let $\phi_0, \phi_1, \cdots, \phi_p$ be an orthonormal base for V such that ϕ_i belongs to the weight Λ_i $(\Lambda_0 = \Lambda)$. Then it is obvious that $\pi(\bar n)\phi_0 - \phi_0$ is orthogonal to ϕ_0 and therefore

$$|\sigma(h\bar n h^{-1})\phi_0|^2 = 1 + \sum_{1 \leqq i \leqq p} \exp\{2\Lambda_i(\log h) - 2\Lambda(\log h)\} |(\phi_i, \pi(\bar n)\phi_0)|^2.$$

---

[28] It is known (see Weyl [8(c)]) that such a representation exists.

Let $\beta_1, \cdots, \beta_q$ be all the distinct roots in P_+ and select $X \in \bar{\mathfrak{n}}_0 = \theta(\mathfrak{n}_0)$ such that $\bar{n} = \exp X$. Then $\pi(\bar{n})\phi_0 - \phi_0 = \sum_{r \geqq 1} \sigma(X^r)\phi_0/r!$ and if $i \neq 0$, $(\phi_i, \pi(\bar{n})\phi_0) = 0$ unless there exist nonnegative integers $m_1, \cdots, m_q$, not all zero, such that $\Lambda_i = \Lambda - (m_1\beta_1 + \cdots + m_q\beta_q)$ on $\mathfrak{h}_{\mathfrak{p}}$. Hence if $a = \min_{1 \leqq i \leqq q} \beta_i(H_0)$, it follows that

$$|\sigma(h_t\bar{n}h_t^{-1})\phi_0|^2 \leqq 1 + \sum_{1 \leqq i \leqq p} e^{-2at} |(\phi_i, \pi(\bar{n})\phi_0)|^2$$

$$\leqq 1 + e^{-2at} |\pi(\bar{n})\phi_0|^2 = 1 + \exp\{2\rho(H(\bar{n})) - 2at\} \qquad (t \geqq 0).$$

This proves that

$$\exp\{2\rho(H(h_t\bar{n}h_t^{-1}))\} \leqq 1 + \exp\{2\rho(H(\bar{n})) - 2at\}$$

and therefore

$$\int e^{-\rho(H(\bar{n}))}\{1 + e^{-2at+2\rho(H(\bar{n}))}\}^{-\frac{1}{2}} d\bar{n} \leqq c(1+t)^d \qquad (t \geqq 0).$$

Now for any integer $r \geqq 0$, let $\bar{N}_r$ denote the set of all points $\bar{n} \in \bar{N}$ where $\rho(H(\bar{n})) \leqq 2^r$. It is obvious from its definition that a is positive. Therefore if $t = 2^r/a$ and $\bar{n} \in \bar{N}_r$, it is clear that $e^{-2at}e^{2\rho(H(\bar{n}))} \leqq 1$ and therefore

$$\int_{\bar{N}_r} e^{-\rho(H(\bar{n}))}\, 2^{-\frac{1}{2}}\, dn \leqq c(1 + a^{-1}2^r)^d.$$

Hence

$$\int_{\bar{N}_r} e^{-\rho(H(\bar{n}))}\, d\bar{n} \leqq c_1 2^{rd} \qquad (r \geqq 0)$$

where $c_1 = 2^{\frac{1}{2}}c(1 + a^{-1})^d$. Let $\bar{N}_{r+1} - \bar{N}_r$ denote the complement of $\bar{N}_r$ in $\bar{N}_{r+1}$. Then if $\epsilon > 0$,

$$\int_{\bar{N}_{r+1}-\bar{N}_r} e^{-\rho(H(\bar{n}))}\{1 + \rho(H(\bar{n}))\}^{-d-\epsilon}\, d\bar{n} \leqq 2^{-r(d+\epsilon)} \int_{\bar{N}_{r+1}} e^{-\rho(H(\bar{n}))}\, d\bar{n} \leqq c_2 2^{-r\epsilon}$$

where $c_2 = 2^d c_1$. Therefore

$$\int_{\bar{N}-\bar{N}_0} e^{-\rho(H(\bar{n}))}\{1 + \rho(H(\bar{n}))\}^{-d-\epsilon}\, d\bar{n} \leqq c_2 \sum_{r \geqq 0} 2^{-r\epsilon} < \infty.$$

Hence in order to complete the proof, it would be sufficient to verify that $\bar{N}_0$ is compact. But this is an immediate consequence of Lemma 40.

COROLLARY. *Let ϵ be a positive number. Then*

$$\int_{\bar{N}} \exp\{-(1+\epsilon)\rho(H(\bar{n}))\} d\bar{n} < \infty.$$

This is obvious because $e^{-\epsilon t}(1+t)^{d-1}$ remains bounded for $t \geqq 0$.

For any $H \in \mathfrak{h}_{\mathfrak{p}}$ we denote by $\operatorname{Re} H$ and $\operatorname{Im} H$ the elements H_1, H_2 respectively in $\mathfrak{h}_{\mathfrak{p}_0}$ such that $H = H_1 + (-1)^{\frac{1}{2}} H_2$.

THEOREM 4. *Define the function* $\mathbf{c}$ *as in Lemma 37 and normalize the Haar measure* $d\bar{n}$ *on* $\bar{N}$ *by the condition*

$$\int_{\bar{N}} e^{-2\rho(H(\bar{n}))}\, d\bar{n} = 1.$$

Then if H' *is an element in* ${}^*\mathfrak{h}_{\mathfrak{p}}'$ *such that* $-\operatorname{Im} H' \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$, *we have the relation*

$$\mathbf{c}(H') = \int_{\bar{N}} \exp\{-(-1)^{\frac{1}{2}}\langle H', H(\bar{n})\rangle - \rho(H(\bar{n}))\}\, d\bar{n}.$$

Put $\nu(H) = (-1)^{\frac{1}{2}}\langle H', H\rangle$ for $H \in \mathfrak{h}_{\mathfrak{p}}$. Then it follows from Lemma 37 and Corollary 1 of Lemma 44 that

$$\sum_{s \in W} \mathbf{c}(sH') e^{-\nu(\log h)} \Phi(sH' : h) = \int_{\bar{N}} \exp\{\nu_-(H(h\bar{n}h^{-1})) - \nu_+(H(\bar{n}))\}\, d\bar{n}$$

for $h \in A_{\mathfrak{p}}(M)$. Select a point $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$ and put $h_t = \exp tH_0$ $(t \geqq 0)$. Then it follows from Corollary 1 of Lemma 35 that the real part of $(-1)^{\frac{1}{2}}\langle sH' - H', H_0\rangle$ is negative if $s \neq 1$ $(s \in W)$. Therefore it is obvious from Lemma 31 that $\lim_{t \to +\infty} e^{-t\nu(H_0)}\Phi(sH' : h_t) = 1$ or 0 according as $s = 1$ or not. Hence

$$\mathbf{c}(H') = \lim_{t \to +\infty} \int_{\bar{N}} \exp\{\nu_-(H(h_t\bar{n}h_t^{-1})) - \nu_+(H(\bar{n}))\}\, d\bar{n}.$$

On the other hand we can evidently choose a positive number $\epsilon < 1$ such that $-\operatorname{Im} H' - \epsilon H_\rho \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$. Put $\nu' = \nu - \epsilon\rho$. Then $\nu_- = \nu' - (1-\epsilon)\rho$, $\nu_+ = \nu' + (1+\epsilon)\rho$ and $\operatorname{Re} \nu'(H) \geqq 0$ for $H \in {}^+\mathfrak{h}_{\mathfrak{p}_0}$. On the other hand

$$\begin{aligned}\nu_-(H(h_t\bar{n}h_t^{-1})) - \nu_+(H(\bar{n})) = \nu'(H(h_t\bar{n}h_t^{-1}) - H(\bar{n})) - (1-\epsilon)\rho(H(h_t\bar{n}h_t^{-1}))\\ - (1+\epsilon)\rho(H(\bar{n})).\end{aligned}$$

Therefore it follows from Lemma 43 that

$$\operatorname{Re}\{\nu_-(H(h_t\bar{n}h_t^{-1})) - \nu_+(H(\bar{n}))\} \leqq -(1+\epsilon)\rho(H(\bar{n}))$$

for $t \geqq 0$. Hence we conclude from the corollary of Lemma 45 that

$$\mathbf{c}(H') = \int_{\bar{N}} \lim_{t \to +\infty} \exp\{\nu_-(H(h_t\bar{n}h_t^{-1})) - \nu_+(H(\bar{n}))\}\, d\bar{n}.$$

Now for a fixed $\bar{n} \in \bar{N}$, select $X \in \bar{\mathfrak{n}}$ such that $\exp X = \bar{n}$. Then $h_t\bar{n}h_t^{-1}$

$=\exp(\mathrm{Ad}(h_t)X)$ and if $X=\sum_{\beta\in P_+} a_\beta X_{-\beta}$ $(a_\beta \in C)$, it is obvious that $\mathrm{Ad}(h_t)X=\sum_\beta a_\beta e^{-t\beta(H_0)}X_{-\beta}$. Since $\beta(H_0)>0$ for every $\beta\in P_+$, it follows that $h_t\bar{n}h_t^{-1}\to 1$ as $t\to+\infty$ and therefore

$$\boldsymbol{c}(H')=\int_{\bar{N}}\exp\{-\nu_+(H(\bar{n}))\}d\bar{n}.$$

This proves the theorem.

We recall that $\mathfrak{h}_{\mathfrak{p}_0}'$ is the set of those points $H\in\mathfrak{h}_{\mathfrak{p}_0}$ where $\alpha(H)\neq 0$ for every $\alpha\in P_+$. We have seen in Section 10 that $\mathfrak{h}_{\mathfrak{p}_0}'\subset {}^*\mathfrak{h}_{\mathfrak{p}_0}'$ and therefore $\boldsymbol{c}$ is defined on $\mathfrak{h}_{\mathfrak{p}_0}'$.

COROLLARY. *Let H_0 be any point in $\mathfrak{h}_{\mathfrak{p}_0}'$. Then*

$$\boldsymbol{c}(H_0)=\operatorname*{Lim}_{\epsilon\to 0}\int_{\bar{N}}\exp\{-(-1)^{\frac{1}{2}}\langle H_0,H(\bar{n})\rangle-(1+\epsilon)\rho(H(\bar{n}))\}d\bar{n}\quad(\epsilon>0).$$

Put $H_\epsilon=H_0-(-1)^{\frac{1}{2}}\epsilon H_\rho$ where ϵ is a positive number. It is obvious that $H_\epsilon\in{}^*\mathfrak{h}_{\mathfrak{p}}'$ and $-\mathrm{Im}\,H_\epsilon\in\mathfrak{h}_{\mathfrak{p}_0}^+$ if ϵ is sufficiently small. Moreover $\boldsymbol{c}(H_0)=\operatorname*{Lim}_{\epsilon\to 0}\boldsymbol{c}(H_\epsilon)$ since $\boldsymbol{c}$ is holomorphic at H_0. Hence the corollary follows immediately from Theorem 4.

We shall now give another interpretation of the above corollary. Let $\mathfrak{D}(\mathfrak{h}_{\mathfrak{p}})$ be the algebra of all polynomial differential operators [5(k), § 2] on $\mathfrak{h}_{\mathfrak{p}}$ and let $\mathcal{B}(\mathfrak{h}_{\mathfrak{p}_0})$ denote the space of all functions on $\mathfrak{h}_{\mathfrak{p}_0}$ of class C^∞ such that Da remains bounded on $\mathfrak{h}_{\mathfrak{p}_0}$ for every $D\in\mathfrak{D}(\mathfrak{h}_{\mathfrak{p}_0})$. We topologize $\mathcal{B}(\mathfrak{h}_{\mathfrak{p}_0})$ in the usual way and consider a $\mathcal{B}$-distribution τ on $\mathfrak{h}_{\mathfrak{p}_0}$ (see [5(k), § 2]). Let dH denote the regular Euclidean measure [5(k), p. 91] on $\mathfrak{h}_{\mathfrak{p}_0}$ and for any $a\in\mathcal{B}(\mathfrak{h}_{\mathfrak{p}_0})$, put

$$a'(H_0)=\int_{\mathfrak{h}_{\mathfrak{p}_0}}\exp\{-(-1)^{\frac{1}{2}}\langle H_0,H\rangle\}a(H)\,dH\qquad(H_0\in\mathfrak{h}_{\mathfrak{p}_0}).$$

Then the Fourier transform of τ is the $\mathcal{B}$-distribution $\bar{\tau}$ given by $\bar{\tau}(a)=\tau(a')$ $(a\in\mathcal{B}(\mathfrak{h}_{\mathfrak{p}_0}))$.

THEOREM 5. *Let $\bar{\tau}$ denote the Fourier transform of the distribution τ defined by*

$$\tau(a)=\int_{\bar{N}}a(H(\bar{n}))e^{-\rho(H(\bar{n}))}\,d\bar{n}\qquad(a\in\mathcal{B}(\mathfrak{h}_{\mathfrak{p}_0})).$$

Then $\bar{\tau}$ coincides on $\mathfrak{h}_{\mathfrak{p}_0}'$ with the analytic function $\boldsymbol{c}$.

We know from Lemma 45 that

$$c=\int_{\bar{N}}e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-r}\,d\bar{n}<\infty,$$

if r is a suitable positive integer. Hence

$$\int_{\bar{N}} |a(H(\bar{n}))|\, e^{-\rho(H(\bar{n}))}\, d\bar{n} \leqq c \sup_{H\in\mathfrak{h}_{\mathfrak{p}_0}} |(1+\rho(H))^r a(H)| \qquad (a\in\mathscr{C}(\mathfrak{h}_{\mathfrak{p}_0}))$$

and therefore τ is a $\mathscr{C}$-distribution. Moreover this inequality implies that

$$\tau(a) = \operatorname*{Lim}_{\epsilon\to 0} \int_{\bar{N}} a(H(\bar{n}))\, e^{-(1+\epsilon)\rho(H(\bar{n}))}\, d\bar{n} \qquad (\epsilon > 0).$$

Now fix an element[17] $a \in C_c^\infty(\mathfrak{h}_{\mathfrak{p}_0}{}')$. Then

$$\bar{\tau}(a) = \operatorname*{Lim}_{\epsilon\to 0} \int_{\bar{N}} a'(H(\bar{n}))\, e^{-(1+\epsilon)\rho(H(\bar{n}))}\, d\bar{n}.$$

On the other hand

$$\int_{\bar{N}} a'(H(\bar{n}))\, e^{-(1+\epsilon)\rho(H(\bar{n}))}\, d\bar{n} = \int_{\bar{N}} e^{-(1+\epsilon)\rho(H(\bar{n}))}\, d\bar{n} \int_{\mathfrak{h}_{\mathfrak{p}_0}} \exp\{-(-1)^{\frac{1}{2}}\langle H(\bar{n}), H\rangle\} a(H)\, dH$$

and it follows from the corollary of Lemma 45 that

$$\int_{\bar{N}} e^{-(1+\epsilon)\rho(H(\bar{n}))}\, d\bar{n} \int_{\mathfrak{h}_{\mathfrak{p}_0}} |a(H)|\, dH < \infty.$$

Therefore by Fubini's Theorem

$$\bar{\tau}(a) = \operatorname*{Lim}_{\epsilon\to 0} \int_{\mathfrak{h}_{\mathfrak{p}_0}} a(H) dH \int_{\bar{N}} \exp\{-(-1)^{\frac{1}{2}}\langle H(\bar{n}), H\rangle - (1+\epsilon)\rho(H(\bar{n}))\} d\bar{n}.$$

Hence if $H_\epsilon = H - (-1)^{\frac{1}{2}}\epsilon H_\rho$, we can conclude from Theorem 4 that

$$\bar{\tau}(a) = \operatorname*{Lim}_{\epsilon\to 0} \int_{\mathfrak{h}_{\mathfrak{p}_0}} a(H)\boldsymbol{c}(H_\epsilon)\, dH.$$

Now let Ω denote the carrier of a. Then Ω is a compact subset of $\mathfrak{h}_{\mathfrak{p}_0}{}'$ and therefore $\boldsymbol{c}$ is holomorphic on some *complex* neighborhood of Ω in $\mathfrak{h}_{\mathfrak{p}}$. Hence it is obvious that

$$\bar{\tau}(a) = \int_{\mathfrak{h}_{\mathfrak{p}_0}} a(H)\boldsymbol{c}(H)\, dH.$$

This proves that $\bar{\tau}$ coincides with $\boldsymbol{c}$ on $\mathfrak{h}_{\mathfrak{p}_0}{}'$.

12. Further study of the function $\boldsymbol{c}$. We shall now investigate the function $\boldsymbol{c}$ a little more closely on $\mathfrak{h}_{\mathfrak{p}_0}{}'$. Let $\mathfrak{F}$ be the space of all linear functions[29] on $\mathfrak{h}_{\mathfrak{p}}$ and $\mathfrak{F}_R$ be the subspace (over R) consisting of the real[8] functions. For any $\lambda \in \mathfrak{F}$, let λ_R and λ_I denote the real and imaginary parts of λ so that $\lambda = \lambda_R + (-1)^{\frac{1}{2}}\lambda_I$ $(\lambda_R, \lambda_I \in \mathfrak{F}_R)$. Then the following lemma establishes an important inequality.

---

[29] Although $\mathfrak{F}$ and $\mathfrak{h}_{\mathfrak{p}}$ have been identified under the bilinear form B, it is sometimes convenient to distinguish between the two.

LEMMA 46. *Put*

$$\psi(\lambda : x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) - \rho(H(xk))\}dk$$

for $\lambda \in \mathfrak{F}$ *and* $x \in G$. *Then for any* $b \in \mathfrak{B}$, *we can select an integer* $d \geqq 0$ *and a positive constant* a *such that*[30]

$$|\psi(\lambda : x ; b)| \leqq a(1 + \|\lambda\|)^d \psi((-1)^{\frac{1}{2}}\lambda_I : x)$$

for all $x \in G$ *and* $\lambda \in \mathfrak{F}$.

Let $\beta_1, \cdots, \beta_r$ be a fundamental system of roots in P. Select linear functions $\Lambda_1, \cdots, \Lambda_r$ on $\mathfrak{h}$ such that[9] $\Lambda_i(H_{\beta_j}) = 2\beta_j(H_{\beta_j})\delta_{ij}$ $(1 \leqq i, j \leqq r)$ where, for any root β, H_β is defined in the same way as in Section 7. Then, by Theorem 1 of [5(b)], there exists an irreducible representation π_i of $\mathfrak{g}$ on a finite-dimensional space V_i with the highest weight Λ_i. Select a unit vector ξ_i in V_i belonging to Λ_i. Extend λ and ρ to linear functions on $\mathfrak{h}$ by defining them to be zero on $\mathfrak{h}_{\mathfrak{k}}$. Then $\lambda = \sum_{1 \leqq i \leqq r} \lambda_i \Lambda_i$ and $\rho = \sum_{1 \leqq i \leqq r} \rho_i \Lambda_i$ where $\lambda_i \in C$ and $\rho_i \in R$. First we shall prove the following result.

LEMMA 47. *Suppose* $\lambda \in \mathfrak{F}$ *and* $x \in G$. *Then*

$$\psi(\lambda : x) = \psi(-\lambda : x^{-1}) = \int_K \prod_{1 \leqq i \leqq r} |\pi_i(x^{-1}k)\xi_i|^{-\nu_i} dk$$

where $\nu_i = (-1)^{\frac{1}{2}}\lambda_i + \rho_i$ $1 \leqq i \leqq r$.

For any $k \in K$, let k_x denote the unique element in K such that $xk \in k_x A_{\mathfrak{p}} N$. Then $k \rightarrow k_x$ is a topological mapping of K onto itself and $dk = \exp\{2\rho(H(xk))\}dk_x$ (see [5(c), p. 241]). Hence

$$\psi(\lambda : x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) + \rho(H(xk))\}dk_x.$$

Replacing k by $k_{x^{-1}}$ in this integral and making use of the relation $H(xk_{x^{-1}}) = -H(x^{-1}k)$ (see [5(c), Lemma 36]), we get

$$\psi(\lambda : x) = \int_K \exp\{-(-1)^{\frac{1}{2}}\lambda(H(x^{-1}k)) - \rho(H(x^{-1}k))\}dk = \psi(-\lambda : x^{-1}).$$

---

[30] In view of the identification of $\mathfrak{F}$ and $\mathfrak{h}_{\mathfrak{p}}$, $\|\lambda\|$ is well-defined $(\lambda \in \mathfrak{F})$.

But $|\pi_i(x^{-1}k)\xi_i| = \exp\{\Lambda_i(H(x^{-1}k))\}$. Hence

$$\psi(-\lambda : x^{-1}) = \int_K \prod_{1 \leqq i \leqq r} |\pi_i(x^{-1}k)\xi_i|^{-\nu_i}\, dk.$$

Now we come to the proof of Lemma 46. Select a base $X_1, \cdots, X_n$ for $\mathfrak{g}_0$ over R and for any $x \in G$ and $t = (t_1, \cdots, t_n) \in R^n$, put $x_t = x\exp(t_1X_1 + \cdots + t_nX_n)$. For any ordered set $M = (m_1, \cdots, m_n)$ of nonnegative integers, we write $|M| = m_1 + \cdots + m_n$, $t^M = t_1^{m_1} \cdots t_n^{m_n}$ and denote by $X(M)$ the coefficient (in $\mathfrak{B}$) of t^M in $(|M|!)^{-1}$ $(t_1X_1 + \cdots + t_nX_n)^{|M|}$. Also put $|t| = \max_{1 \leqq i \leqq n} |t_i|$ and $M + M' = (m_1 + m_1', \cdots, m_n + m_n')$ if $M' = (m_1', \cdots, m_n')$. Let E_j be the space of all endomorphisms of V_j $(1 \leqq j \leqq r)$. For any $T \in E_j$, put $|T| = \sup_{|v| \leqq 1} |Tv|$ $(v \in V_j)$. Then E_j is a Banach space under this norm and

$$\pi_j(\exp\{-(t_1X_1 + \cdots + t_nX_n)\}) = \sum_M t^M(-1)^{|M|}\pi_j(X(M)),$$

the series converging absolutely and uniformly in E_j (see [5(c), § 5]) provided $|t|$ remains bounded. Define $\tilde{\theta}$ as in Section 5 and let $b \to b^*$ $(b \in \mathfrak{B})$ be the anti-automorphism of $\mathfrak{B}$ over R which coincides with $-\tilde{\theta}$ on $\mathfrak{g}$. Then it is clear that $\pi_j(b^*)$ is the adjoint of $\pi_j(b)$ (in the sense of Hilbert space theory). Put

$$b_M = \sum_{M_1+M_2=M} (-1)^{|M|}(X(M_1))^*X(M_2)$$

for any M. Then it is obvious that

$$|\pi_j(x_t^{-1}k)\xi_j|^2 = |\pi_j(x^{-1}k)\xi_j|^2 + \sum_{|M| \geqq 1} t^M(\pi_j(x^{-1}k)\xi_j, \pi_j(b_M)\pi_j(x^{-1}k)\xi_j)$$

for all k, x and t $(1 \leqq j \leqq r)$. Put

$$\Psi_{M,j}(x) = |\pi_j(x)\xi_j|^{-2}(\pi_j(x)\xi_j, \pi_j(b_M)\pi_j(x)\xi_j) \qquad (x \in G).$$

Then $|\Psi_{M,j}(x)| \leqq |\pi_j(b_M|$. Hence $\Psi_{M,j}$ is a bounded analytic function on G and

$$|\pi_j(x_t^{-1}k)\xi_j|^2 = |\pi_j(x^{-1}k)\xi_j|^2\{1 + \sum_{|M| \geqq 1} t^M\Psi_{M,j}(x^{-1}k)\}.$$

Obviously this series converges uniformly with respect to x, k and t provided x varies within a compact subset of G and $|t|$ remains bounded. Therefore by the binomial theorem,

$$\begin{aligned}\exp\{-(-1)^{\frac{1}{2}}\lambda(H(x_t^{-1}k)) - \rho(H(x_t^{-1}k))\} &= \prod_{1 \leqq j \leqq r} |\pi_j(x_t^{-1}k)\xi_j|^{-\nu_j} \\ &= \exp\{-(-1)^{\frac{1}{2}}\lambda(H(x^{-1}k)) - \rho(H(x^{-1}k))\} \sum_M t^M\Psi_M(x^{-1}k : \lambda)\end{aligned}$$

provides $|t|$ is sufficiently small. Here $\Psi_M(x:\lambda)$ is a function on $G \times \mathfrak{F}$ which can be written as a polynomial in ν_j and $\Psi_{M',j}$ $(1 \leqq j \leqq r, |M'| \leqq |M|)$ with constant coefficients. Therefore it is clear that there exists a positive number a_M and an integer $d_M \geqq 0$ such that

$$|\Psi_M(x:\lambda)| \leqq a_M(1+\|\lambda\|)^{d_M} \qquad (x \in G, \lambda \in \mathfrak{F}).$$

Moreover it is obvious that for a fixed x, the above series converges uniformly with respect to k and t provided $|t|$ is sufficiently small. Therefore by integrating over K, we get an expansion of $\psi(-\lambda:x_t^{-1}) = \psi(\lambda:x_t)$ in powers of $t_1, \cdots, t_n$. This shows that if $M = (m_1, \cdots, m_n)$,

$$\psi(\lambda:x;X(M)) = (m_1!\cdots m_n!)^{-1}\{\partial^{m_1+\cdots+m_n}/\partial t_1^{m_1}\cdots\partial t_n^{m_n})\psi(\lambda:x_t)\}_{t=0}$$

$$= \int_K \Psi_M(x^{-1}k:\lambda)\exp\{-(-1)^{\frac{1}{2}}\lambda(H(x^{-1}k)) - \rho(H(x^{-1}k))\}dk.$$

Hence

$$|\psi(\lambda:x;X(M))| \leqq a_M(1+\|\lambda\|)^{d_M}\psi((-1)^{\frac{1}{2}}\lambda_I:x)$$

and the assertion of the lemma follows from the fact that the elements $X(M)$ form a base for $\mathfrak{B}$.

The following result will be needed in another paper.

LEMMA 48. *Let Ω be a compact set in G. Then we can select a positive number c such that $\psi(0:xy) \leqq c\psi(0:x)$ for all $x \in G$ and $y \in \Omega$.*

It is clear that

$$e^{-\rho(H(y^{-1}x^{-1}k))} = \prod_{1\leqq j\leqq r} |\pi_j(y^{-1}x^{-1}k)\xi_j|^{-\rho_j}$$

and

$$|\pi_j(y)|^{-1}|\pi_j(x^{-1}k)\xi_j| \leqq |\pi_j(y^{-1}x^{-1}k)\xi_j| \leqq |\pi_j(y^{-1})|\,|\pi_j(x^{-1}k)\xi_j|.$$

Therefore if we put

$$c = \sup_{y\in\Omega} \prod_{1\leqq j\leqq r} \{|\pi_j(y)|^{\rho_j} + |\pi_j(y^{-1})|^{-\rho_j}\},$$

it follows that

$$e^{-\rho(H(y^{-1}x^{-1}k))} \leqq ce^{-\rho(H(x^{-1}k))}$$

for $y \in \Omega$. In view of Lemma 47 our assertion is now obvious.

Now for any positive number ϵ, let $\mathfrak{F}_\epsilon$ denote the open neighborhood of $\mathfrak{F}_R$ in $\mathfrak{F}$ consisting of those points $\lambda \in \mathfrak{F}$ for which[27] $|\operatorname{Im}\lambda_j| < \epsilon/2$ $(1 \leqq j \leqq r)$. Then it follows from Lemmas 2 and 35 and Corollary 2 of Lemma 35 that

$$|\lambda_I(H(hk))| \leqq \tfrac{1}{2}\epsilon \sum_{1\leqq j\leqq r} |\Lambda_j(H(hk))|$$

$$\leqq \tfrac{1}{2}\epsilon \sum_{1\leqq j\leqq r} \Lambda_j(\log h + \log h^*) = \epsilon\rho(\log h) \qquad (h \in \mathrm{Cl}(A_\mathfrak{p}^+)),$$

since[31] $\sum_{1\leqq j\leqq r} \Lambda_j = \frac{1}{2}\sum_{\beta\in P}\beta$ and $\rho(\log h^*) = \rho(\log h)$. Therefore we get the following result.

LEMMA 49. *Suppose* $\lambda \in \mathfrak{F}_\epsilon$ *and* $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$. *Then*

$$\psi((-1)^{\frac{1}{2}}\lambda_I : h) \leqq e^{\epsilon\rho(\log h)}\psi(0:h).$$

Lemmas 46 and 49, together with Theorem 3, give us an estimate for $\psi(\lambda:h;b)$ which will be of great value in the discussion below.

Select $u_1, \cdots, u_w \in \mathfrak{H}_\mathfrak{p}$ as in the corollary of Lemma 8 and put

$$\psi_i(\lambda:H) = e^{\rho(H)}\psi(\lambda:\exp H; u_i') \qquad (\lambda\in\mathfrak{F}, H\in\mathfrak{h}_{\mathfrak{k}_0}, 1\leqq i\leqq w)$$

where $u_i' = e^\rho u_i \circ e^{-\rho}$. Fix an element $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}^-$ and let $\Psi(\lambda:t)$ $(t\in R)$ denote the one-column matrix $\psi_i(\lambda:tH_0)$ $1\leqq i\leqq w$. Let us consider $d\Psi/dt$. Choose $q_{ij}\in I_\mathfrak{g}$ such that $H_0u_j = \sum_{1\leqq i\leqq w} u_i\gamma(q_{ij})$ $(1\leqq j\leqq w)$. Then if $h_t = \exp tH_0$ $(t\in R)$, it follows from Theorem 2 and Lemmas 18 and 23 that

$$d\psi_j(\lambda:tH_0)/dt = \sum_{1\leqq i\leqq w} \psi_i(\lambda:tH_0)\gamma(q_{ij}:(-1)^{\frac{1}{2}}\lambda) + \theta_j(\lambda:h_t) \qquad (t\geqq 1)$$

where

$$\theta_j(\lambda:h) = \sum_{1\leqq i\leqq w}\sum_{1\leqq k\leqq s} g_{jik}(h)\psi_i(\lambda:\log h)\gamma(q_{jik}:(-1)^{\frac{1}{2}}\lambda) \qquad (\lambda\in\mathfrak{F}, h\in A_\mathfrak{p}^+),$$

$g_{jik}\in\mathfrak{R}$, $q_{jik}\in I_\mathfrak{g}$ and s is a positive integer. Put $\beta(H_0 = \min_{\alpha\in P_+}\alpha(H_0)$. Then it is obvious that for any $g\in\mathfrak{R}$, there exists a positive number c such that $|g(h_t)| \leqq ce^{-2t\beta(H_0)}$ $(t\geqq 1)$. Let $\Theta(\lambda:t)$ denote the one-column matrix $\theta_i(\lambda:h_t)$ $1\leqq i\leqq w$ and put $\|a\| = (\sum_{1\leqq i\leqq m}\sum_{1\leqq j\leqq n}|a_{ij}|^2)^{\frac{1}{2}}$ for any $m\times n$ matrix $a = (a_{ij})$ with complex coefficients. Then it follows from Lemmas 46 and 49 and Theorem 3 that

$$\|\Theta(\lambda:t)\| \leqq c_1\exp\{\epsilon t\rho(H_0) - 2t\beta(H_0)\}(1+\|\lambda\|)^{d_1}t^{d_1}$$

for $t\geqq 1$ and $\lambda\in\mathfrak{F}_\epsilon$. Here c_1 is a positive number and d_1 a nonnegative integer. Let $\Xi(\lambda)$ denote the $w\times w$ matrix given by $\Xi_{ij}(\lambda) = \gamma(q_{ji}:(-1)^{\frac{1}{2}}\lambda)$

---

[31] Put $\Lambda = \frac{1}{2}\sum_{\beta\in P}\beta$. Then $2\Lambda(H_{\beta_j}) = \beta_j(H_{\beta_j})$ for $1\leqq j\leqq r$ (see Weyl [8(c)]). Hence $\Lambda = \Lambda_1 + \cdots + \Lambda_r$.

$(1 \leqq i, j \leqq w)$. Then the above equation can be written in matrix notation as follows:

$$d\Psi(\lambda : t)/dt = \Xi(\lambda)\Psi(\lambda : t) + \Theta(\lambda : t) \qquad (t \geqq 1).$$

Now put $\Psi_0(\lambda : t) = \exp(-t\Xi(\lambda))\Psi(\lambda : t)$ and $\Theta_0(\lambda : t) = \exp(-t\Xi(\lambda))\Theta(\lambda : t)$. Then it is clear that

$$d\Psi_0(\lambda : t)/dt = \Theta_0(\lambda : t) \qquad (t \geqq 1).$$

We shall now estimate $\| \Theta_0(\lambda : t) \|$. It is obvious from the definition of $\Xi(\lambda)$ that

$$H_0 u_j \equiv \sum_{1 \leqq i \leqq w} \Xi_{ji}(\lambda) u_i \bmod SJ_{\lambda^*}$$

in the notation of Section 3, if we put $\lambda^* = (-1)^{\frac{1}{2}}\lambda$. Hence we conclude from Corollary 2 of Lemma 14 that $\lambda^*(sH_0)$ $(s \in W)$ are all the eigenvalues of $\Xi(\lambda)$. Put $\tau(\lambda) = 2w \max_{s \in W} | \lambda_I(sH_0) |$. Then it follows from Lemma 60 of the Appendix that

$$\| \exp(-t\Xi(\lambda)) \| \leqq e^{t\tau(\lambda)} w^{\frac{1}{2}} \sum_{0 \leqq k < w} t^k \| \Xi(\lambda) \|^k \qquad (t > 0).$$

Therefore since $\| \Theta_0(\lambda : t) \| \leqq \| \exp(-t\Xi(\lambda)) \| \, \| \Theta(\lambda : t) \|$, it is obvious that there exists a positive number c_2 and an integer $d_2 \geqq 0$ such that

$$\| \Theta_0(\lambda : t) \| \leqq c_2(1 + \| \lambda \|)^{d_2} t^{d_2} \exp\{\tau(\lambda)t + \epsilon t\rho(H_0) - 2t\beta(H_0)\}$$

for $\lambda \in \mathfrak{F}_\epsilon$ and $t \geqq 1$. Moreover by choosing ϵ sufficiently small, we can obviously arrange that $\beta(H_0) \geqq \tau(\lambda) + \epsilon\rho(H_0)$ for all $\lambda \in \mathfrak{F}_\epsilon$. Then in this case

$$\| \Theta_0(\lambda : t) \| \leqq c_2(1 + \| \lambda \|)^{d_2} t^{d_2} e^{-t\beta(H_0)} \qquad (t \geqq 1, \lambda \in \mathfrak{F}_\epsilon).$$

This shows that the integral $\int_1^\infty \| \Theta_0(\lambda : t) \| \, dt$ converges uniformly with respect to λ as λ varies in a compact subset of $\mathfrak{F}_\epsilon$. Moreover there exists a positive number c_3 such that

$$\int_1^\infty \| \Theta_0(\lambda : t) \| \, dt \leqq c_3(1 + \| \lambda \|)^{d_2} \qquad (\lambda \in \mathfrak{F}_\epsilon).$$

But since $d\Psi_0(\lambda : t)/dt = \Theta_0(\lambda : t)$, this implies that $\Psi_0(\lambda : t)$ tends to a limit as $t \to +\infty$. If we denote this limit by $\Psi_0(\lambda : \infty)$, we have the relation

$$\Psi_0(\lambda : \infty) = \Psi_0(\lambda : 1) + \int_1^\infty \Theta_0(\lambda : t) \, dt \qquad (\lambda \in \mathfrak{F}_\epsilon).$$

In view of the uniform convergence of the integral, it is clear that $\Psi_0(\lambda:\infty)$ is a holomorphic (matrix-) function of λ on $\mathfrak{F}_\epsilon$. Moreover since $\|\Psi_0(\lambda:1)\| \leqq \|\exp(-\Xi(\lambda))\|\,\|\Psi(\lambda:1)\|$, it follows without difficulty (by making use of Lemmas 46 and 49 and the above estimate for $\|\exp(-\Xi(\lambda))\|$) that $\|\Psi_0(\lambda:1)\| \leqq c_4(1+\|\lambda\|)^{d_4}$ for suitable positive numbers c_4, d_4. Therefore $\|\Psi_0(\lambda:\infty)\| \leqq c_5(1+\|\lambda\|)^{d_5}$ $(\lambda \in \mathfrak{F}_\epsilon)$ for an appropriate choice of c_5, d_5. Hence if we apply Lemma 58 of the Appendix to $V=\mathfrak{F}_{\epsilon/2}$, we get the following result.

LEMMA 50. *If ϵ is sufficiently small, there exists an integer $d \geqq 0$ with the following property. For any $u \in S(\mathfrak{h}_\mathfrak{p})$, the function*

$$(1+\|\lambda\|)^{-d}\,\|\Psi_0(\lambda;\partial(u):\infty)\|$$

remains bounded as λ varies in $\mathfrak{F}_\epsilon$.

Now define π as in Lemma 11 and let $\mathfrak{F}_\epsilon'$ denote the set of those elements $\lambda \in \mathfrak{F}_\epsilon$ where $\pi(\lambda) \neq 0$. We may assume that ϵ is so small that $\|\lambda_I\| < \|\Lambda\|/2$ for any $\lambda \in \mathfrak{F}_\epsilon$ and $\Lambda \in L'$ (see Section 8 for the definition of L'). Then it follows without difficulty that $\mathfrak{F}_\epsilon \subset {}^*\mathfrak{h}_\mathfrak{p}$ and therefore $\mathfrak{F}_\epsilon' \subset {}^*\mathfrak{h}_\mathfrak{p}'$. Hence if $\lambda \in \mathfrak{F}_\epsilon'$, we conclude from Lemma 37 that

$$\psi_i(\lambda:tH_0) = \sum_{s\in W} c(s\lambda)\Phi(s\lambda:h_t;u_i) \qquad (1 \leqq i \leqq w,\ t > M)$$

where M is a suitable positive number. Define $e_{sH} \in S(\mathfrak{h}_\mathfrak{p})$ $(s \in W, H \in \mathfrak{h}_\mathfrak{p})$ as in Lemma 14 and put $e_s = e_{s\lambda^*}$. Moreover define the $w \times w$ matrix $E(s)$ as follows:

$$e_s u_i \equiv \sum_{1\leqq j\leqq w} E_{ij}(s)u_j \bmod SJ_{\lambda^*} \qquad (E_{ij}(s) \in C).$$

Then it follows from Lemma 14 that $\sum_{s\in W} \epsilon(s)E(s) = \pi(\lambda^*)I$ where I is the unit matrix. Moreover $e_sH_0 = H_0e_s \equiv \lambda^*(s^{-1}H_0)e_s \bmod SJ_{\lambda^*}$ by the same lemma and therefore

$$E(s)\Xi(\lambda) = \Xi(\lambda)E(s) = \lambda^*(s^{-1}H_0)E(s).$$

Hence

$$\begin{aligned}\pi(\lambda^*)\Psi_0(\lambda:t) &= \sum_{s\in W} \epsilon(s)E(s)\exp(-t\Xi(\lambda))\Psi(\lambda:t)\\ &= \sum_{s\in W} \epsilon(s)\exp\{-\lambda^*(s^{-1}H_0)t\}E(s)\Psi(\lambda:t).\end{aligned}$$

Now put $\xi(\mu:h) = \exp\{\mu^*(\log h)\}$ $(\mu \in \mathfrak{F}, h \in A_\mathfrak{p})$ where $\mu^* = (-1)^{\frac{1}{2}}\mu$. Then it is obvious that $\xi(\mu:h;u) = u(\mu^*)\xi(\mu:h)$ for $u \in \mathfrak{H}_\mathfrak{p}$ and therefore $\xi(\mu:h;u) = 0$ for $u \in SJ_{\mu^*}$. Also

$$\sum_{1 \leqq j \leqq w} E_{ij}(s) u_j \equiv e_s u_i \equiv u_i(s\lambda^*) e_s \bmod SJ_\lambda. \qquad (1 \leqq i \leqq w)$$

from Lemma 14. Therefore

$$\sum_{1 \leqq j \leqq w} E_{ij}(s) \xi(s'\lambda : h ; u_j) = u_i(s\lambda^*) e_s(s'\lambda^*) \xi(s'\lambda : h) \qquad (s, s' \in W).$$

Hence it follows from the third statement of Lemma 14 that

$$\sum_j E_{ij}(s) \xi(s'\lambda : h ; u_j) = \begin{cases} 0 \text{ if } s \neq s' \\ u_i(s\lambda^*) \epsilon(s) \pi(\lambda^*) \xi(s\lambda : h) \text{ if } s = s'. \end{cases}$$

Let $\psi_{0j}(\lambda : \infty)$ $(1 \leqq j \leqq w)$ denote the coefficients of the one-column matrix $\Psi_0(\lambda : \infty)$. Then

$$\pi(\lambda^*) \psi_{0i}(\lambda : \infty) = \operatorname*{Lim}_{t \to +\infty} \sum_{s, s' \in W} \sum_j \epsilon(s) \xi(s\lambda : h_t^{-1}) E_{ij}(s) \boldsymbol{c}(s'\lambda) \Phi(s'\lambda : h_t ; u_j).$$

But since $\beta(H_0) \geqq \tau(\lambda) + \epsilon\rho(H_0)$, it follows that $|\lambda_I(sH_0)| - \beta(H_0) \leqq -\epsilon\rho(H_0)$ for $s \in W$. Therefore it is obvious that

$$\operatorname*{Lim}_{t \to +\infty} |\Phi(s'\lambda : h_t ; u_j) - \xi(s'\lambda : h_t ; u_j)| = 0 \qquad (s' \in W)$$

and hence

$$\begin{aligned} \pi(\lambda^*) \psi_{0i}(\lambda : \infty) &= \operatorname*{Lim}_{t \to +\infty} \sum_{s, s' \in W} \sum_j \epsilon(s) \xi(s\lambda : h_t^{-1}) E_{ij}(s) \boldsymbol{c}(s'\lambda) \xi(s'\lambda : h_t ; u_j) \\ &= \pi(\lambda^*) \operatorname*{Lim}_{t \to +\infty} \sum_{s \in W} \xi(s\lambda : h_t^{-1}) \boldsymbol{c}(s\lambda) u_i(s\lambda^*) \xi(s\lambda : h_t) \\ &= \pi(\lambda^*) \sum_{s \in W} u_i(s\lambda^*) \boldsymbol{c}(s\lambda) \end{aligned}$$

in view of what we have said above. Thus we have obtained the following result.

LEMMA 51. $\psi_{0i}(\lambda : \infty) = \sum_{s \in W} u_i(s\lambda^*) \boldsymbol{c}(s\lambda)$ *for any* $\lambda \in \mathfrak{F}_\epsilon'$.

Define σ^i $(1 \leqq i \leqq w)$ as in Lemma 14.

COROLLARY. $\sum_{1 \leqq i \leqq w} \sigma^i(\lambda^*) \psi_{0i}(\lambda : \infty) = \pi(\lambda^*) \boldsymbol{c}(\lambda)$ *for* $\lambda \in \mathfrak{F}_\epsilon'$.

This follows immediately from the above lemma and the third statement of Lemma 14.

We have seen that $\Psi_0(\lambda : \infty)$ is a holomorphic function of λ on $\mathfrak{F}_\epsilon$. Therefore in view of the above corollary and Lemma 50, we have the following result.

LEMMA 52. *Suppose* ϵ *is sufficiently small. Then there exists a holomorphic function* $\boldsymbol{b}$ *on* $\mathfrak{F}_\epsilon$ *such that* $\boldsymbol{b}(\lambda) = \pi(\lambda) \boldsymbol{c}(\lambda)$ *for* $\lambda \in \mathfrak{F}_\epsilon'$. *Moreover* *we can select an integer* $d \geqq 0$ *with the property that for any* $u \in S(\mathfrak{h}_\mathfrak{p})$, $(1+\|\lambda\|)^{-d}|\boldsymbol{b}(\lambda;\partial(u))|$ *remains bounded as* λ *varies in* $\mathfrak{F}_\epsilon$.

Define the $\mathscr{C}$-distributions τ and $\bar{\tau}$ on $\mathfrak{h}_{\mathfrak{p}_0}$ as in Theorem 5.

COROLLARY. *The distribution* $\pi\bar{\tau}$ *coincides on* $\mathfrak{h}_{\mathfrak{p}_0}$ *with* $\boldsymbol{b}$.

We use the notation of the proof of Theorem 5. It is sufficient to show that

$$\bar{\tau}(\pi a) = \int_{\mathfrak{h}_{\mathfrak{p}_0}} \boldsymbol{b}(H)a(H)\,dH$$

for any $a \in C_c^\infty(\mathfrak{h}_{\mathfrak{p}_0})$. Put $H_\epsilon = H - (-1)^{\frac{1}{2}}\epsilon H_\rho$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$ where ϵ is a positive number. Then it is obvious that $\pi(H_\epsilon) \neq 0$. Hence if ϵ is sufficiently small, $H_\epsilon \in {}^*\mathfrak{h}_\mathfrak{p}'$ and therefore $\boldsymbol{c}(H_\epsilon)$ is well-defined for all $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Moreover if we use the method of proof of Theorem 5, it follows without difficulty that

$$\bar{\tau}(\pi a) = \operatorname*{Lim}_{\epsilon\to 0}\int_{\mathfrak{h}_{\mathfrak{p}_0}} a(H)\pi(H)\boldsymbol{c}(H_\epsilon)\,dH.$$

On the other hand it is obvious that $|\alpha(H)| \leqq |\alpha(H_\epsilon)|$ for $\alpha \in \Sigma$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$ and therefore $|\pi(H)\boldsymbol{c}(H_\epsilon)| \leqq |\boldsymbol{b}(H_\epsilon)|$. Let Ω be the carrier of a. Then since Ω is compact and since $\boldsymbol{b}$ is holomorphic on a complex neighborhood of $\mathfrak{h}_{\mathfrak{p}_0}$ in $\mathfrak{h}_\mathfrak{p}$, it is obvious that $|\boldsymbol{b}(H_\epsilon)|$ remains uniformly bounded for all sufficiently small values of ϵ as H varies in Ω. Hence we conclude that

$$\bar{\tau}(\pi a) = \int_{\mathfrak{h}_{\mathfrak{p}_0}} \operatorname*{Lim}_{\epsilon\to 0}\{a(H)\pi(H)\boldsymbol{c}(H_\epsilon)\}\,dH.$$

But it is obvious that $\operatorname*{Lim}_{\epsilon\to 0}\pi(H)\boldsymbol{c}(H_\epsilon) = \boldsymbol{b}(H)$ if $\pi(H) \neq 0$. Therefore

$$\bar{\tau}(\pi a) = \int_{\mathfrak{h}_{\mathfrak{p}_0}} a(H)\boldsymbol{b}(H)\,dH$$

and this proves the corollary.

13. The case $l = 1$. We assume in this section that[32] $\dim \mathfrak{h}_\mathfrak{p} = 1$. Then[16] we can select $\alpha \in \Sigma$ such that 2α is the only other possible element in Σ. Let p and q denote the number of roots in P_+ which coincide on $\mathfrak{h}_\mathfrak{p}$ with α and 2α respectively. Then $\rho = \frac{1}{2}(p+2q)\alpha$. Let H be the element in $\mathfrak{h}_\mathfrak{p}$ such that $\alpha(H) = 1$. Then $\langle H, H\rangle = 2\sum_{\beta\in P_+}\beta(H)^2 = 2(p+4q)$. This implies that $H_\alpha = (2p+8q)^{-1}H$ and $H_\rho = \frac{1}{2}(p+2q)H_\alpha$. Hence it follows from Lemma 27 that

---

[32] A special case of this type has been discussed by Bargmann [1]. We follow the same method.

$$2(p+4q)\delta'(\omega) = H^2 + (p+2q)H + \{2p(e^{2\alpha}-1)^{-1} + 4q(e^{4\alpha}-1)^{-1}\}H.$$

Put $t(h) = \alpha(\log h)$ for $h \in A_{\mathfrak{p}}$. Then t can be regarded as the coordinate function on the one-dimensional Lie group $A_{\mathfrak{p}}$ and so it is clear that

$$\begin{aligned}2(p+4q)\delta'(\omega) &= d^2/dt^2 + \{p\coth t + 2q\coth 2t\}d/dt \\ &= d^2/dt^2 + \{(p+q)\coth t + q\tanh t\}d/dt,\end{aligned}$$

since $\coth 2t = \frac{1}{2}(\coth t + \tanh t)$. Now put $z = -(\sinh t)^2$. Then the above relation becomes

$$\tfrac{1}{2}(p+4q)\delta'(\omega) = z(z-1)d^2/dz^2 + \tfrac{1}{2}\{(p+2q+2)z - (p+q+1)\}d/dz.$$

On the other hand if λ is any linear function on $\mathfrak{h}_{\mathfrak{p}}$, we know from Corollary 2 of Lemma 27 that

$$\gamma(\omega:(-1)^{\frac{1}{2}}\lambda) = -\langle\lambda,\lambda\rangle - \langle\rho,\rho\rangle = -\tfrac{1}{2}(p+4q)^{-1}\{\lambda(H)^2 + \rho(H)^2\}.$$

Therefore if we put $\phi_\lambda(h) = \psi(\lambda:h)$ $(h \in A_{\mathfrak{p}})$, it follows from Lemma 18 that

$$\begin{aligned}&z(z-1)d^2\phi_\lambda/dz^2 \\ &+ \tfrac{1}{2}\{(p+2q+2)z - (p+q+1)\}d\phi_\lambda/dz + \tfrac{1}{4}\{\lambda(H)^2 + (\tfrac{1}{2}p+q)^2\}\phi_\lambda = 0.\end{aligned}$$

Now let

$$a = \{p+2q+2\lambda^*(H)\}/4, \quad b = \{p+2q-2\lambda^*(H)\}/4, \quad c = (p+q+1)/2$$

where $\lambda^* = (-1)^{\frac{1}{2}}\lambda$. Then the above equation becomes

$$z(z-1)d^2\phi_\lambda/dz^2 + \{(a+b+1)z - c\}d\phi_\lambda/dz + ab\phi_\lambda = 0.$$

Now z can be regarded as a coördinate function on $A_{\mathfrak{p}}^+$. Therefore $\phi_\lambda = g(z)$ where g is analytic function on the interval $-\infty < z < 0$. Moreover $W = \{1, s\}$ where $sH = -H$. Therefore $\phi_\lambda(h) = \phi_\lambda(h^s) = \phi_\lambda(h^{-1})$ $(h \in A_{\mathfrak{p}})$ and so ϕ_λ can be expanded in powers of t^2 in the neighborhood of the point $h = 1$. But this implies that g is actually analytic also at $z = 0$. Moreover $g(0) = \phi_\lambda(1) = 1$. Therefore since $c > 0$, it follows by a direct substitution of the power series for g around the origin, in the above differential equation, that $g(z)$ is the hypergeometric function $F(a,b,c,z)$. But it is known (see Bargmann [1, p. 627]) that

$$F(a,b,c,z)=|z|^{-a}\Gamma(c)\Gamma(b-a)\{\Gamma(b)\Gamma(c-a)\}^{-1}F(a,1+a-c,1+a-b,z^{-1})$$
$$+|z|^{-b}\Gamma(c)\Gamma(a-b)\{\Gamma(b)\Gamma(c-b)\}^{-1}F(b,1+b-c,1+b-a,z^{-1})$$
$$(z<0)$$

provided $a-b=\lambda^*(H)$ is not an integer. (Here Γ denotes the classical Gamma function.) Therefore if λ is real, it is clear that

$$\lim_{t'\to+\infty}|e^{t'\rho(H)}\phi_\lambda(\exp t'H)-\boldsymbol{c}(\lambda)e^{t'\lambda^*(H)}-\boldsymbol{c}(-\lambda)e^{-t'\lambda^*(H)}|=0$$

where

$$\boldsymbol{c}(\lambda)=\Gamma(\tfrac{1}{2}(p+q+1))\Gamma(\lambda^*(H))$$
$$\times\{\Gamma(4^{-1}(p+2q+2\lambda^*(H)))\Gamma(4^{-1}(p+2+2\lambda^*(H)))\}^{-1}.$$

Moreover in the present case $\pi=\alpha$ and therefore

$$\pi(\lambda)=\lambda(H_\alpha)=(2p+8q)^{-1}\lambda(H).$$

Hence

$$(-1)^{\frac{1}{2}}\boldsymbol{b}(\lambda)=(2p+8q)^{-1}\Gamma((p+q+1)/2)\Gamma(1+\lambda^*(H))$$
$$\times\{\Gamma((p+2q+2\lambda^*(H))/4)\Gamma((p+2+2\lambda^*(H))/4)\}^{-1},$$

and by analytic continuation this formula holds for all $\lambda\in\mathfrak{F}_\epsilon$ if ϵ is sufficiently small. Moreover if $\lambda\in\mathfrak{F}_R$, it is obvious that $|\boldsymbol{b}(-\lambda)|=|\boldsymbol{b}(\lambda)|$. Hence we have obtained the following result.

LEMMA 53. *If ϵ is sufficiently small, $\boldsymbol{b}$ is never zero on $\mathfrak{F}_\epsilon$. Moreover $|\boldsymbol{b}(s'\lambda)|=|\boldsymbol{b}(\lambda)|$ for $s'\in W$ and $\lambda\in\mathfrak{F}_R$.*

We shall see in another paper that a similar result holds when $l>1$.

14. The complex case.[33] In this section we assume that G is a *complex* group. Then it follows easily (see [5(f), p. 513]) that no root $\alpha\in P$ can vanish identically either on $\mathfrak{h}_\mathfrak{p}$ or on $\mathfrak{h}_\mathfrak{k}$. Moreover the restrictions on $\mathfrak{h}_\mathfrak{p}$ of two distinct roots $\alpha,\beta\in P$, are linearly independent unless $\beta=-\theta\alpha$. Hence $P=P_+$ and we can select a subset Q of P such that exactly one of the two roots $\alpha,-\theta\alpha$ lies in Q for any $\alpha\in P$. Put $d(H)=\prod_{\alpha\in Q}(e^{\alpha(H)}-e^{-\alpha(H)})$ $(H\in\mathfrak{h}_\mathfrak{p})$. It is obvious that $\pi(H)=\prod_{\alpha\in Q}\alpha(H)$ and therefore $d(sH)=\epsilon(s)d(H)$

---

[33] After this paper had been written, two recent notes of F. A. Beresin (Doklady Akad. Nauk. SSSR N. S., vol. 107 (1956), pp. 9-12, vol. 110 (1956), pp. 897-900) came to my attention. The results of this section are also contained in these notes.

$(s \in W)$. Moreover $\rho(H) = \frac{1}{2} \sum_{\alpha \in P} \alpha(H) = \sum_{\alpha \in Q} \alpha(H)$. Hence it follows by elementary considerations of divisibility (see Weyl [8(b)]) that

$$d(H) = \sum_{s \in W} \epsilon(s) e^{\rho(s^{-1}H)} \qquad (H \in \mathfrak{h}_\mathfrak{p}).$$

Now put $D(h) = d(\log h)$ for $h \in A_\mathfrak{p}$ and let us use the notation of Section 7. Then it is obvious[22] that $\varpi D = \langle \rho, \rho \rangle D$. If we take this fact and Lemma 27 into account, a simple calculation gives the following result.

LEMMA 54. *$\delta'(\omega) = D^{-1}\gamma(\omega) \circ D$ in the present case.*

Fix $H' \in \mathfrak{h}_\mathfrak{p}$ and consider the function

$$F(H' : h) = D(h)^{-1} \exp\{\rho(\log h) + \langle H', \log h \rangle\}$$

$(h \in A_\mathfrak{p}^+)$ on $A_\mathfrak{p}^+$. In view of the above lemma, F is an eigenfunction of the operator $\delta'(\omega)$ and the corresponding eigenvalue is $\gamma'(\omega : H')$. Moreover $D(h)^{-1} e^{\rho(\log h)} = \prod_{\alpha \in Q} \{1 - e^{-2\alpha(\log h)}\}^{-1}$. Therefore it follows easily from the reasoning of Section 8 that $\Phi' = F$ in the notation of Lemma 29. Now put

$$\phi_\lambda(x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) - \rho(H(xk))\} dk \qquad (x \in G, \lambda \in \mathfrak{F})$$

and fix $\lambda \in \mathfrak{F}_R' = \mathfrak{h}_{\mathfrak{p}_0}'$. Then it follows from Lemma 37 that[34]

$$D(h)\phi_\lambda(h) = \sum_{s \in W} \boldsymbol{c}(s\lambda) \exp\{s\lambda^*(\log h)\} \qquad (h \in A_\mathfrak{p}(M))$$

where $\lambda^* = (-1)^{\frac{1}{2}}\lambda$. However since both sides are analytic functions on $A_\mathfrak{p}$ this equation must hold for all $h \in A_\mathfrak{p}$. On the other hand $\phi_\lambda(h^s) = \phi_\lambda(h)$ while $D(h^s) = \epsilon(s) D(h)$. Therefore since the points $s\lambda$ $(s \in W)$ are all distinct, it follows (see [5(b), Lemma 41]) that $\boldsymbol{c}(s\lambda) = \epsilon(s)\boldsymbol{c}(\lambda)$. Hence

$$D(h)\phi_\lambda(h) = \boldsymbol{c}(\lambda) \sum_{s \in W} \epsilon(s) \exp\{s\lambda^*(\log h)\} \qquad (h \in A_\mathfrak{p}).$$

Now π, being an element in $\mathfrak{H}_\mathfrak{p}$, can be considered as a differential operator on $A_\mathfrak{p}$. In view of the expression for D obtained earlier, it is clear that $D(1 ; \pi) = w\pi(\rho)$ where w is the order of W. Hence if we apply the operator π to the above equation and put $h = 1$, we get

$$w\pi(\rho) = w\boldsymbol{c}(\lambda)\pi(\lambda^*)$$

since $\phi_\lambda(1) = 1$. Hence

$$\pi(\lambda) D(h) \phi_\lambda(h)$$
$$= (-1)^{-q/2}\pi(\rho) \sum_{s \in W} \epsilon(s) \exp\{(-1)^{\frac{1}{2}} s\lambda(\log h)\} \qquad (h \in A_\mathfrak{p})$$

---

[34] $s\mu(H)$ denotes the value of $s\mu$ at H $(s \in W, \mu \in \mathfrak{F}, H \in \mathfrak{h}_\mathfrak{p})$.

where q is the number of roots in Q. However both sides are holomorphic functions of λ on $\mathfrak{F}$ and so the above equation must hold for all $\lambda \in \mathfrak{F}$. Thus we have obtained another proof of an earlier result (see [5(e), Theorem 7]). Also $\boldsymbol{b}(\lambda) = (-1)^{-q/2}\pi(\rho)$. This shows that $\boldsymbol{b}$ is a constant in this case.

It is interesting to note that from the above results one can deduce the following extension of Lemma 54, which we state here without proof.[35]

LEMMA 55. $\delta'(q) = D^{-1}\gamma(q) \circ D$ *for every* $q \in I_{\mathfrak{g}}$.

15. Appendix. LEMMA 56. *Let t be a real variable and $k_1, \cdots, k_r$ distinct real numbers. Then*

$$\operatorname*{Lim\,sup}_{t \to +\infty} \Big| \sum_{1 \leqq i \leqq r} c_i \exp\{(-1)^{\frac{1}{2}} k_i t\} \Big| \geqq \Big\{ \sum_{1 \leqq i \leqq r} |c_i|^2 \Big\}^{\frac{1}{2}}$$

for any complex numbers $c_1, \cdots, c_r$.

Put $f(t) = \sum_i c_i \exp\{(-1)^{\frac{1}{2}} k_i t\}$. Then it follows by direct computation that

$$\operatorname*{Lim}_{T \to +\infty} T^{-1} \int_0^T |f(t)|^2 \, dt = \sum_i |c_i|^2.$$

On the other hand if $a = \operatorname*{Lim\,sup}_{t \to +\infty} |f(t)|$, it is obvious that

$$\operatorname*{Lim}_{T \to +\infty} T^{-1} \int_0^T |f(t)|^2 \, dt \leqq a^2.$$

Therefore $a^2 \geqq \sum_i |c_i|^2$.

COROLLARY. *Let $k_1, \cdots, k_r$ be nonzero complex numbers and $p_0, p_1, \cdots, p_r$ polynomials in t with complex coefficients. Suppose*

$$\operatorname*{Lim\,sup}_{t \to +\infty} |p_0(t) + p_1(t) e^{k_1 t} + \cdots + p_r(t) e^{k_r t}| \leqq a$$

for some real number a. Then p_0 is a constant and $|p_0| \leqq a$.

Let l_i denote the real part of k_i. If $l_i < 0$, it is obvious that $\operatorname*{Lim}_{t \to +\infty} |p_i(t) e^{k_i t}| = 0$. Therefore if we suppose that $l_i \geqq 0$ for $1 \leqq i \leqq s$ while $l_i < 0$ for $i > s$, it follows that

$$\operatorname*{Lim\,sup}_{t \to +\infty} |p_0(t) + \sum_{1 \leqq i \leqq s} p_i(t) e^{k_i t}| \leqq a.$$

---

[35] Cf. Theorem 2 of [5(g)]

Hence without loss of generality we may assume that $s = r$ and $k_1, \cdots, k_r$ are distinct and $p_i \neq 0$ $(0 \leqq i \leqq r)$. We shall now first show that $l_1 = l_2 = \cdots = l_r = 0$. For otherwise suppose $l = \max(l_1, \cdots, l_r) > 0$. We may assume that $l_1 = l_2 = \cdots = l_j = l$ while $l_i < l$ for $i > j$. Let n be the highest among the degrees of $p_1, \cdots, p_j$ and put $c_i' = \lim_{t \to +\infty} p_i(t)/t^n$. Then $c_1', \cdots, c_j'$ cannot all be zero and it is clear that

$$0 = \limsup_{t \to +\infty} t^{-n} e^{-lt} \mid p_0(t) + p_1(t) e^{k_1 t} + \cdots + p_r(t) e^{k_r t} \mid$$

$$= \limsup_{t \to +\infty} \mid c_1' e^{(k_1 - l)t} + c_2' e^{(k_2 - l)t} + \cdots + c_j' e^{(k_j - l)t} \mid.$$

But since $k_i - l$ $(1 \leqq i \leqq j)$ are distinct pure imaginary numbers, we get a contradiction with Lemma 56. This proves that $l = 0$.

Now let m be the maximum of the degrees of $p_0, p_1, \cdots, p_r$. We claim $m = 0$. For otherwise since $l_i = 0$ $1 \leqq i \leqq r$, it follows that

$$\lim_{t \to +\infty} t^{-m} \mid p_0(t) + \sum_{1 \leqq i \leqq r} p_i(t) e^{k_i t} \mid = 0.$$

This implies that

$$\lim_{t \to +\infty} \mid c_0 + \sum_{1 \leqq i \leqq r} c_i e^{k_i t} \mid = 0$$

where $c_i = \lim_{t \to +\infty} p_i(t)/t^m$ $(0 \leqq i \leqq r)$. But in view of the definition of $m, c_0, \cdots, c_r$ cannot all be zero and so again we get a contradiction with the above lemma. This shows that $m = 0$ and hence $p_0, \cdots, p_r$ are all constants. Therefore again by the above lemma, $|p_0| \leqq a$.

Let E be a vector space over R of finite dimension. We shall say that a subset F of E is *full* if $tH \in F$ whenever $H \in F$ and $t \geqq 1$ $(t \in R)$.

LEMMA 57. *Let* $k_i \neq 0$ $(1 \leqq i \leqq r)$ *be a finite set of linear functions*[36] *and* $p_0, \cdots, p_r$ *polynomial functions on* E. *Suppose* V *is a nonempty, open and full subset of* E *and* a *a real number such that*

$$| p_0(H) + p_1(H) e^{k_1(H)} + \cdots + p_r(H) e^{k_r(H)} | \leqq a$$

for all $H \in V$. *Then* p_0 *is a constant and* $|p_0| \leqq a$.

Let m be the degree of p_0. Since V is open, we can select $H_0 \in V$ in such a way that $k_i(H_0) \neq 0$ $(1 \leqq i \leqq r)$ and $q_0(t) = p_0(tH_0)$ is a polynomial of degree m in the real variable t. Put $q_i(t) = p_i(tH_0)$ and $k_i' = k_i(H_0)$ $1 \leqq i \leqq r$. Then since $tH_0 \in V$ for $t \geqq 1$, it follows that

$$| q_0(t) + q_1(t) e^{k_1' t} + \cdots + q_r(t) e^{k_r' t} | \leqq a \qquad (t \geqq 1).$$

---

[36] We permit linear or polynomial functions on E to take complex values.

Hence we conclude from the corollary of Lemma 56 that q_0 is a constant and $|q_0| \leqq a$. This proves that $m = 0$ and therefore $|p_0| = |q_0| \leqq a$.

COROLLARY. *Let k_i $(i \geqq 1)$ be a sequence of distinct linear functions and p_i $(i \geqq 1)$ a sequence of polynomial functions on E and V a nonempty, open and full subset of E. Suppose the following two conditions hold.*

(1) *For each linear function k on E the series*

$$\sum_{1 \leqq i < \infty} |p_i(H)\exp(k(H) + k_i(H))|$$

converges uniformly for $H \in V$.

(2) $\sum_{1 \leqq i < \infty} p_i(H) e^{k_i(H)} = 0$ *for $H \in V$.*

Then $p_i = 0$ for every i.

For otherwise select an index j such that $p_j \neq 0$. For a given $\epsilon > 0$, choose an integer $N \geqq j$ such that

$$\sum_{i > N} |p_i(H)\exp(k_i(H) - k_j(H))| \leqq \epsilon$$

for all $H \in V$. This is possible by condition (1). Moreover it is obvious from condition (2) that

$$\left| \sum_{1 \leqq i \leqq N} p_i(H)\exp(k_i(H) - k_j(H)) \right| \leqq \epsilon \qquad (H \in V).$$

On the other hand $k_i - k_j \neq 0$ for $i \neq j$ and so we conclude from the above lemma that p_j is a constant and $|p_j| \leqq \epsilon$. But ϵ being arbitrary, this implies that $p_j = 0$. As this contradicts the choice of j, our assertion is proved.

Let $(z_1, \cdots, z_l)$ denote the Cartesian coordinates of a point z in the complex Euclidean space C^l of dimension l. We regard C^l as a vector space over C in the usual way and put $|z| = \max_{1 \leqq i \leqq l} |z_i|$. The distance between two sets U and V in C^l is defined to be $\inf |z - \zeta|$ $(z \in U, \zeta \in V)$.

LEMMA 58. *Let U be an open set in C^l and V a subset of U and let ϵ denote the distance between V and the complement of U in C^l. Then if ξ is any holomorphic function on U,*

$$\sup_{z \in V} |(\partial^{k_1 + \cdots + k_l}/\partial z_1^{k_1} \cdots \partial z_l^{k_l})\xi(z)| \leqq k_1! k_2! \cdots k_l! (2\pi/\epsilon)^{k_1 + \cdots + k_l} \sup_{z \in U} |\xi(z)|$$

for any integers $k_1, \cdots, k_l \geqq 0$.

We may obviously assume that $\epsilon > 0$. Let ϵ' be any positive number less than ϵ. Then if $z \in V$ and $|z - \zeta| \leqq \epsilon'$, it follows that $\zeta \in U$. Hence

$$(\partial^{k_1+\cdots+k_l}/\partial z_1^{k_1}\cdots\partial z_l^{k_l})\xi(z)$$
$$= k_1!\cdots k_l!\{2\pi(-1)^{\frac{1}{2}}\}^{-1}\oint_1\cdots\oint_l \xi(\zeta)\{(\zeta_1 - z_1)^{k_1+1}\cdots(\zeta_l - z_l)^{k_l+1}\}^{-1} \times d\zeta_1\cdots d\zeta_l$$

where $\oint_i$ denotes complex integration with respect to ζ_i on the circle $|z_i - \zeta_i| = \epsilon'$. Therefore it is obvious that

$$|(\partial^{k_1+\cdots+k_l}/\partial z_1^{k_1}\cdots\partial z_l^{k_l})\xi(z)| \leqq k_1!\cdots k_l! \sup_{\zeta\in U}|\xi(\zeta)|\,\epsilon'^{-k}(2\pi)^{k-1}$$

where $k = k_i + \cdots + k_l$. This being true for every $\epsilon' < \epsilon$, our assertion now follows immediately.

The following lemma and its corollary will be needed in another paper.

LEMMA 59. *Suppose* ϵ *is positive in Lemma* 57 *and* $\eta = z_1\xi$. *Then if* $\sup_{z\in U}(1 + |z|)^{-d}|\eta(z)| < \infty$ *for some integer* $d \geqq 0$, *we can conclude that* $\sup_{z\in V}(1 + |z|)^{-d}|\xi(z)| < \infty$.

Select a positive number $\epsilon' < \min(1/6, \epsilon/3)$ and let V' be the set of those points $z \in V$ where $|z_1| < \epsilon'$. Obviously it would be enough to verify that $\sup_{z\in V'}(1 + |z|)^{-d}|\xi(z)| < \infty$. Now fix a point $z^0 = (z_1^0, z_2^0, \cdots, z_l^0)$ in V'. Then

$$\xi(z^0) = (2\pi(-1)^{\frac{1}{2}})^{-1}\oint z_1^{-1}\eta(z_1, z_2^0, \cdots z_l^0)(z_1 - z_1^0)^{-1}dz_1$$

where $\oint$ denotes complex integration over the circle $|z_1| = 2\epsilon'$ in the z_1-plane. Now let $z' = (z_1, z_2^0, \cdots, z_l^0)$ where $|z_1| = 2\epsilon'$. Then it is clear that

$$1 + |z^0| \geqq 1 + |z'| - 3\epsilon' \geqq \tfrac{1}{2}(1 + |z'|).$$

Hence it follows that

$$(1 + |z^0|)^{-d}|\xi(z^0)| \leqq (2^d/\epsilon')\sup_{z\in U}(1 + |z|)^{-d}|\eta(z)|.$$

This proves the lemma.

COROLLARY. *Let* p *be a polynomial function on* C^l *which can be written as a product of linear factors. Then the above lemma also holds if* $\eta = p\xi$.

This follows by an easy induction on the degree of p.

For any $m \times m$ matrix $\Lambda = (\lambda_{ij})_{1 \leqq i, j \leqq m}$ (with complex coefficients) put $\| \Lambda \| = (\sum_{i,j} | \lambda_{ij} |^2)^{\frac{1}{2}}$.

LEMMA 60. *Let* Λ *be an* $m \times m$ *matrix and let* $\lambda_1, \cdots, \lambda_m$ *denote all the eigenvalues of* Λ. *Put* $\nu = \max_{1 \leqq i \leqq m} | \operatorname{Re} \lambda_i |$. *Then*

$$\| e^{\Lambda} \| \leqq m^{\frac{1}{2}} e^{2m\nu} \sum_{0 \leqq k < m} \| \Lambda \|^k.$$

It is well known that we can find a unitary matrix U such that $\Lambda' = U \Lambda U^{-1}$ has zeros everywhere below the diagonal. Since Λ and Λ' have the same eigenvalues and $\| \Lambda' \| = \| \Lambda \|$, $\| e^{\Lambda'} \| = \| e^{\Lambda} \|$, we may replace Λ by Λ' in our problem. Therefore we can assume that $\Lambda = A + N$ where A is a diagonal and N a supertriangular[37] matrix. Now consider $e^{t\Lambda} = e^{t(A+N)}$ $(t \in R)$ and put $n(t) = e^{-tA} e^{t(A+N)}$. Then it is clear that

$$\begin{aligned} dn(t)/dt &= e^{-tA}(-A) e^{t(A+N)} + e^{-tA}(A+N) e^{t(A+N)} \\ &= e^{-tA} N e^{t(A+N)} = e^{-tA} N e^{tA} n(t). \end{aligned}$$

This differential equation can be solved by the method of iteration and one finds that

$$n(t) = 1 + \sum_{k \geqq 1} \int_{0 \leqq \tau_1 \leqq \tau_2 \leqq \cdots \leqq \tau_k \leqq t} N(\tau_k) N(\tau_{k-1}) \cdots N(\tau_1) \, d\tau_1 \cdots d\tau_k$$

for $t \geqq 0$. Here 1 stands for the unit matrix and $N(\tau) = e^{-\tau A} N e^{\tau A}$ $(\tau \in R)$. But since $N(\tau)$ is also supertriangular, the product $N(\tau_k) \cdots N(\tau_1)$ is zero if $k \geqq m$. Moreover $A = A_1 + (-1)^{\frac{1}{2}} A_2$ where A_1, A_2 are both diagonal and real. Then since $e^{(-1)^{\frac{1}{2}} \tau A_2}$ is unitary, it follows that

$$\| N(\tau) \| = \| e^{-\tau A_1} N e^{\tau A_1} \| \qquad (\tau \in R).$$

But the diagonal elements of A are exactly the eigenvalues of Λ. Therefore if $| \tau | \leqq 1$, no coefficient of $e^{\tau A_1}$ can exceed e^{ν} in absolutee value. Hence $\| N(\tau) \| \leqq e^{2\nu} \| N \|$ for $| \tau | \leqq 1$. This shows that

$$\int_{0 \leqq \tau_1 \leqq \cdots \leqq \tau_k \leqq t} \| N(\tau_k) \cdots N(\tau_1) \| \, d\tau_1 \cdots d\tau_k \leqq \| N \|^k e^{2k\nu}$$

for $0 \leqq t \leqq 1$ and $k \geqq 1$. Therefore

$$\| n(1) \| \leqq \| 1 \| + \sum_{1 \leqq k < m} \| N \|^k e^{2k\nu}.$$

---

[37] This means that all the coefficients of N on or below the diagonal are zero.

But $e^{\Lambda} = e^{A} n(1)$ and so $\| e^{\Lambda} \| \leqq e^{\nu} \| n(1) \|$. Moreover $\| \Lambda \|^2 = \| A \|^2 + \| N \|^2 \geqq \| N \|^2$. Therefore

$$\begin{aligned} \| e^{\Lambda} \| \leqq e^{\nu} \| n(1) \| &\leqq m^{\frac{1}{2}} e^{2m\nu} \sum_{0 \leqq k < m} \| N \|^k \\ &\leqq m^{\frac{1}{2}} e^{2m\nu} \sum_{0 \leqq k < m} \| \Lambda \|^k \end{aligned}$$

since $\| 1 \| = m^{\frac{1}{2}}$.

COLUMBIA UNIVERSITY.

REFERENCES.

[1] V. Bargmann, *Ann. of Math.*, vol. 48 (1947), pp. 568-640.

[2] E. Cartan, *Ann. École Norm. Sup.*, vol. 44 (1927), pp. 345-467.

[3] C. Chevalley, a) *Introduction to the theory of algebraic functions of one variable*, American Mathematical Society, 1951.
b) *Amer. Jour. Math.*, vol. 77 (1955), pp. 778-782.

[4] R. Godement, *Trans. Amer. Math. Soc.*, vol. 73 (1953), pp. 496-556.

[5] Harish-Chandra, a) *Ann. of Math.*, vol. 50 (1949), pp. 900-915.
b) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
c) " " " " vol. 75 (1953), pp. 185-243.
d) " " " " vol. 76 (1954), pp. 26-65.
e) " " " " vol. 76 (1954), pp. 234-253.
f) " " " " vol. 76 (1954), pp. 485-528.
g) " " " " vol. 83 (1956), pp. 98-163.
h) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
i) " " " vol. 78 (1956), pp. 1-41.
j) " " " vol. 78 (1956), pp. 564-628.
k) " " " vol. 79 (1957), pp. 87-120.
l) " " " vol. 79 (1957), pp. 193-257.
m) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 40 (1954), pp. 200-204.
n) " " " " " vol. 43 (1957), pp. 408-409.

[6] K. Iwasawa, *Ann. of Math.*, vol. 50 (1949), pp. 507-557.

[7] G. D. Mostow, *Bull. Amer. Math. Soc.*, vol. 55 (1949), pp. 969-980.

[8] H. Weyl, a) *Math. Ann.*, vol. 68 (1910), pp. 220-269.
b) *Math. Zeit.*, vol. 24 (1925), pp. 328-395.
c) *The structure and representations of continuous groups*, Princeton, The Institute for Advanced Study, 1935.

INTERSECTION MULTIPLICITIES OF MAXIMAL CONNECTED BUNCHES.*

By J. P. Murre.

Introduction. It is possible to use the connectedness of the total transform of a simple point for a birational transformation as a starting point for the theory of intersection multiplicities. As explained in [VI] page 249, it is then possible to attach an integer, not only to a proper component of intersection, but also to every maximal connected** bunch in the intersection of two varieties of complementary dimensions on a complete ambient variety (subject to some restrictions on this ambient variety). In this paper such an integer is defined, provided the ambient variety is projective and *every point* of the bunch under consideration is simple on the ambient variety.

The technique used to derive from the connectedness theorem ([II], [VIII] and [IX]) the theory of intersection multiplicities is essentially the method of Severi [IV] and van der Waerden [V].†). The elimination of all the arbitrary elements entering into this method is based upon a certain commutativity argument (see § 2) which is, essentially, also contained in [V] (cf. page 639). It is assumed that the multiplicity for proper components is already defined (we proceed by induction on the excess of the bunch, see § 2).

The terminology and notations are from [VI].

1. Preparations. Let A^a be a variety in projective N-space P^N, defined over a field k. Let t_{ij}, $j=0,1,\cdots,N$, be $(N+1)^2$ independent transcendentals over k. Consider the projective transformation of P^N, the matrix of which is $T=(t_{ij})$. Since the t_{ij} are independent transcendentals over k, we shall say that this projective transformation *is generic over k*. Let (x) be a generic point of A over $k(t)$, consider the locus A^T of the point $(y)=T^{-1}(x)$ over $k(t)$ (this locus exists since $k(t,y)/k(t)=k(t,x)/k(t)$

---

* Received December 15, 1956; revised January 20, 1958.

** For the meaning of the term "connected" we refer to [II], No. 1 or we take the usual definition in topology for the Zariski topology.

† Mr. J. de Boer has kindly informed me that W. L. Chow has also defined and studied the intersection multipilicty for maximal connected bunches by methods similar to those of Severi and van der Waerden.

is regular). It is easily checked that if $F_i(X)=0$, $i=1,2,\cdots$ is a system of equations for A over k, then $F_i(TX)=0$, $i=1,2,\cdots$ is a system of equations for A^T over $k(t)$; hence if a point $Q\in A^T$ then $TQ\in A$, and conversely. Clearly A^T is the transform of A by T^{-1} (hence, in particular, $\deg. A^T=\deg. A=g$). In [V], § 2, it is shown that there exists a (singular) matrix T' such that A^T specializes (as a cycle) to $\sum_{i=1}^{g} L_i$ over the specialization $T\to T'$ with reference to k, where every L_i is an a-dimensional linear space generic over k, $L_i\neq L_j$ for $i\neq j$, and $\bigcap_i L_i$ is an $(a-1)$-dimensional linear space generic over k. From this, one obtains by the theory of specializations of cycles (cf. [III], page 104, § 7), the following lemma:

LEMMA 1. *Let A^a and B^b be varieties in projective N-space ($N\leqq a+b$), defined over a field k. Let T be a projective transformation generic over k. Then*

i. *$A^T\cdot B$ is defined and $A^T\cdot B=\sum_i C_i$ with $C_i\neq C_j$ for $i\neq j$* [i. e., $i(A^T\cdot B, C_i; P^N)=1$].

ii. *A generic point of C_i over a field of definition for C_i is generic on B over k.*

If $A=\sum_i n_i A_i$ is a projective cycle, rational over k, and if T is a projective transformation, generic over k, then we define $A^T=\sum_i n_i A_i{}^T$.

LEMMA 2. *Let A^a and B^b be k-prime rational cycles in projective N-space ($N\leqq a+b$), with reduced expressions $A=\sum_i A_i$ and $B=\sum_i B_i$* (i. e., *the coefficients are* 1). *Let T be a projective transformation generic over k. Then we have $A^T\cdot B=\sum_i C_i$, $C_i\neq C_j$ for $i\neq j$, and $\sum_i C_i$ is $k(t)$-prime rational. Furthermore, a generic point of C_i over a field of definition for C_i is generic on B over k.*

Proof. It follows by Lemma 1**i.** that $A^T\cdot B$ is defined. Consider first $A_i{}^T\cdot B_j=\sum_h C_{ijh}$. Assume now that $C_{i_0j_0h_0}=C_{i_1j_1h_1}$. It follows from Lemma 1**ii.** that $j_0=j_1$. Let U be the inverse transformation of T; clearly U is generic over k. From our preceding remarks, it follows that $A_i\cdot B_j{}^U=\sum_h C_{ijh}{}^U$. Again by Lemma 1**ii.**, it follows that $i_0=i_1$; then by Lemma 1**i.**, $h_0=h_1$. Therefore $A^T\cdot B=\sum_i C_i$, $C_i\neq C_j$ for $i\neq j$. Clearly $\sum_i C_i$ is $k(t)$-rational; hence we only need show that the C_i are conjugate to each other over $k(t)$. Consider (cf. [V], page 627) the cycle W in $P^N\times P^N\times P^{N^2+2N}$, which is the locus of (P,Q,S) over k, where P and Q are independent generic points of A and B over k and where $P=SQ$ (S is interpreted as an $(N+1)$-square matrix, hence as a projective transformation in P^N). Let X_i, resp. X'_i, $(i=0,\cdots,N)$ be corresponding projective coordinates in the first and second projective space P^N and let Y_{ij} $(i,j=0,\cdots,N)$ be projective coordinates in P^{N^2+2N}. The following equations are among the equations for W

$$X_i(\sum_{j=0}^{N} Y_{0j}X'_j) - X_0(\sum_{j=0}^{N} Y_{ij}X'_j) = 0, \qquad i=1,\cdots,N. \tag{1}$$

If $P=(p_0,\cdots,p_N)$ and $Q=(q_0,\cdots,q_N)$, then we can assume that $p_0\neq 0$ and $q_0\neq 0$. It follows easily that the s_{ij} with $j\neq 0$ and s_{00} can be taken as independent transcendentals over $k(P,Q)$, the $s_{i0}(i\neq 0)$ being then uniquely determined by (1). It follows in particular that dim. $W=a+b+N^2+N$. Let R_i be a generic point of C_i over the algebraic closure of $k(t)$; it can be assumed that the X_0-coordinate of the R_i and the TR_i are different from zero for all i. TR_i being in A, it follows that $(P,Q)\rightarrow(TR_i,R_i)$ over k, and then by the equations (1), $(P,Q,S)\rightarrow 2(TR_i,R_i,T)$ over k (as follows from the preceding remarks about the s_{ij}). Since R_i has the dimension $a+b-N$ over $k(t)$, it follows for dimension reasons that the specialization is generic. Hence $R_i\rightarrow R_j$ over $k(t)$, and conversely. This completes the proof since the assertion on the generic points follows from Lemma 1**ii.**

Again, let A^a be a variety in projective N-space, defined over k. Let L^t be a linear variety such that $L^t\cap A=\phi$. We will denote the *projecting cone* through A with L^t as center of projection by $\Gamma_{(A,L)}$. The letter Γ will be reserved for varieties of this type. If k' is a field of definition for A and L, then $\Gamma_{(A,L)}$ is the locus over k' of a point T which is on the line T_1T_2 generic over the field $k'(T_1,T_2)$, where T_1 and T_2 are independent generic points of A and L over k'. In [I], page 154, $\Gamma_{(A,L)}$ is called the *cross-join* of A and L. In the following, we assume L generic over k and $t<N-a$. We will use the following two properties, the proofs of which are omitted (see [I], page 154, Lemma 1): **a.** $\Gamma_{(A,L)}$ is a variety of dimension $a+t+1$; **b.** if S is a simple point on A such that L is still generic over $k(S)$, then S is simple on $\Gamma_{(A,L)}$ and the tangent space to $\Gamma_{(A,L)}$ at S is spanned by the tangent space to A at S and L. Furthermore, we note that (as follows from the definition of $\Gamma_{(A,L)}$) if T' is a point on $\Gamma_{(A,L)}$ and if $T'\notin A$, then there is a point $T'_1\in A$ such that the line $T'T'_1$ meets L.

The following lemma is essentially well-known (cf. [I], page 170, Lemmas IV and V).

LEMMA 3. *Let A^a be a simple subvariety of a variety V^n in projective N-space, let A and V be defined over a field k. Let L^{N-n-1} be a linear space generic over k. Then we have (if $\Gamma=\Gamma_{(A,L)}$):*

i. $\Gamma \cdot V = A + \sum_\lambda \eta_\lambda A_\lambda$, *and every* A_λ *is simple on* V.

ii. *if* B^b *is any simple subvariety defined over* k, *then every component* C *of* $A_\lambda \cap B$, *not contained in* $A \cap B$, *is proper, and a generic point of* C *over a field of definition for* C *is generic on* B *over* k.

iii. *if* C *is any simple subvariety of* V, *algebraic over* k, *then there is a point of* C *not in any* A_λ (*this implies that, if* D *is a component of* $A_\lambda \cap B$, *contained in a component* C *of* $A \cap B$ *simple on* V, *then* D *is strictly contained in* C).

Proof. Let K be the compositum of the smallest field of definition for L and k. Let A_λ be a component of $\Gamma \cap V$ of dimension a', we shall show $a' \leqq a$. Assume $a' > a$. Let M^{N-a-1} be a linear space generic over K, let K_1 be the algebraic closure of the smallest field of definition for M containing k. By [VII], Lemma 1, $M \cdot V = V_1^{n-a-1}$, where V_1 is a variety. Furthermore, $M \cap A = \phi$ for dimension reasons (hence $V_1 \cap A = \phi$). Let R_1 and R_2 be independent generic points of V_1 and A over K_1, let R be a point on the line R_1R_2 generic over the field $K_1(R_1, R_2)$. Let X be the locus of R over K_1 (X is the cross-join of A and V_1, see [I], page 154). Clearly $\dim. X \leqq n$. Since $\dim. A_\lambda > a$, it follows that there is a point $R'_1 \in A_\lambda \cap M$, hence $R'_1 \in V_1$ and $R'_1 \notin A$. Now $R'_1 \in \Gamma$, $R'_1 \notin A$, hence there is a point $R'_2 \in A$ such that the line $R'_1R'_2$ meets the linear variety L^{N-n-1}. However, $R'_1R'_2$ is on X, hence $X \cap L \neq \phi$. X is a variety of dimension not greater than n, defined over a field K_1, and L^{N-n-1} is generic over K_1; hence $X \cap L = \phi$. Contradiction. Hence $\dim. A_\lambda \leqq a$. By [VI], Chap. VI, Cor. 1 of Th. 1 it follows that $\dim. A_\lambda \geqq a$. Hence $\dim. A_\lambda = a$. It follows that A is a component of $\Gamma \cap V$; $i(\Gamma \cdot V, A; P^N) = 1$ follows by applying [VI], Chap. VI, Th. 6 to Γ and V and to the tangent spaces to Γ and V at a generic point of A over K; those tangent spaces have the tangent space to A at this point as intersection (by **b.**), and therefore they are transversal. This completes part of the proof of **i.**

Next, let B^b be any simple subvariety of V, defined over k. Let S be a generic point over the algebraic closure of K of a component C of $A_\lambda \cap B$. Let $S \notin A$. There is a point $S' \in A$ such that $S \in \Gamma_{(S',L)}$. Let H be a hyperplane, containing L and not going through S and S', let k_1 be the smallest field of definition for H containing k. The coordinates in P^N being $H, X, \cdots, X_N$; L is defined by the equations $H = 0$, $\sum_{j=1}^{N} v_{ij} X_j = 0$ $(i = 1, \cdots, n)$, v_{ij} independent transcendentals over k_1. Introduce the affine space $S_H^N = P^N - H$. Consider in $S_H^N \times S_H^N$ the variety $A' \times B'$, where A' and B'

are the affine varieties corresponding to A and B respectively, and the linear variety Λ^{2N-n} defined by the equations $\sum_{j=1}^{N} v_{ij}(X_j - x'_j) = 0$, $i = 1, \cdots, n$, where $S' = (1, x'_1, \cdots, x'_N)$.[1] Let $S = (1, x_1, \cdots, x_N)$. Then since $S \neq S'$, there is a j such that $x'_j \neq x_j$; let $x'_1 \neq x_1$. Let k_2 be the field obtained by adjoining to k_1 all the v_{ij} except the v_{1j} (for all j). Then $K = k_1(v) = k_2(v)$ is contained in $k_2(x, x')$; in fact, we have the following inclusions: $k \subset k_1 \subset k_2 \subset K \subset k_2(x, x')$. Since $S' \times S \in A' \times B'$ and $\dim.(A' \times B') = a + b$, we have $\dim._{k_2} k_2(x, x') \leqq a + b$; furthermore, by [VI], Chap. V, Prop. 1, $\dim._K K(x, x') \geqq a + b - n$. Combining, we obtain

$$a + b \geqq \dim._{k_2} k_2(x, x') = \dim._{k_2} K + \dim._K K(x, x') \geqq n + (a + b - n).$$

Therefore $\dim._{k_2} k_2(x, x') = a + b$; hence $\dim._{k_2} k_2(x) = b$, i.e., $S = (x)$ is generic on B over k_2 (so a foritori over k). Furthermore, $\dim._K K(x, x') = a + b - n$; hence $\dim._K K(x)$ (which by [VI], Chap. VI, Cor. 1 of Th. 1 is at least $a + b - n$, since S is simple on V) is $a + b - n$, i.e., C is a proper component of $A_\lambda \cap B$ on V. This completes the proof of **ii.**, and if we take for B the variety V itself, then also the remaining part of **i.** is proved.

Next let C be any simple subvariety of V, algebraic over k. Let Q be a point of C, simple on V and algebraic over k. We will show $Q \notin A_\lambda$. Let $Q \in A_\lambda$. Let Q_1 be a generic point of A_λ over K, $Q_1 \notin A$; hence there is a point $P \in A$ such that the line PQ_1 meets L, i.e., $P \in \Gamma_{(Q_1, L)} \cap V$. Since L is generic over $k(Q)$, it follows that (if we apply **i.** to V, $A = Q_1$ and L) $\Gamma_{(Q_1, L)} \cdot V = Q_1 + P + \sum_{i=2}^{h} Q_i$ with $Q_i \neq Q_1$ for $i \neq 1$. Since $\Gamma_{(Q_1, L)} = \Gamma_{(P, L)}$, it follows that Q_1 is algebraic over $K(P)$; hence L is generic over $k(P)$, i.e. $\Gamma_{(P, L)} \cdot V = P + \sum_{i=1}^{h} Q_i$ with $Q_i \neq P$ (again by **i.**). Let $(Q_1, P) \rightarrow (Q, P')$ over K. Then we still have that $Q \in \Gamma_{(P', L)} \cap V$ (by [III], page 53g). Assume first that $Q \neq P'$. Again let H be a hyperplane, containing L, but not going through Q and P'. Write $Q = (1, y_1, \cdots, y_N)$ and $P' = (1, y'_1, \cdots, y'_N)$. Since we can assume that A is different from V (if $A = V$ then there is no A_λ), we have $\dim._{k_1} k_1(P') < n$ (the notations are as above). However, since Q is algebraic over $k \subset k_1$, it follows that the n equations (for $\Gamma_{(P', L)}$) $\sum_{j=1}^{N} v_{ij}(X_j - y'_j) = 0$, $i = 1, \cdots, n$, cannot be fulfilled by Q since the v_{ij} are independent transcendentals over k_1. Next assume $Q = P'$. The tangent spaces to V at $Q = P'$ and $\Gamma_{(Q,L)}$ are transversal (their intersection is the point Q, for otherwise the tangent space to V at Q which is of dimension n and algebraic over k would meet the linear space L^{N-n-1} which is generic over k). From this, it follows by [VI], Chap. VI, Th. 6 that $Q = P'$ is a proper component of multiplicity 1 of $\Gamma_{(P',L)} \cap V$. On the other hand, consider a specialization $(P, \sum_{i=1}^{h} Q_i) \rightarrow (P', Q + \sum_{i=2}^{h} Q'_i)$ over K. Consider the variety V and the linear varieties $\Gamma_{(P,L)}$ and $\Gamma_{(P',L)}$. It follows easily by [VI], Chap. V, Cor. 1 of Th. 3 that the proper component $P' = Q$ of $\Gamma_{(P',L)} \cap V$ has a multiplicity greater than 1. Contradiction. Hence $Q \notin A_\lambda$.

---

[1] $\Gamma_{(S', L)}$ is then defined by the equations $\sum_{j=1}^{N} v_{ij}(X_j - x_j'H) = 0$, $i = 1, \cdots, n$, hence $S' \times S \in \Lambda$.

The following is the main result of this section.

PROPOSITION 1.** *Let A^a be a simple subvariety of a projective variety V^n. Let k be a field of definition for A and V. Then there exists a variety U, a variety $W \subset U \times V$, for U and W an algebraically closed field of definition K containing k, and a point Q' simple on U and algebraic over K, such that the following is true: if B^b $(a + b \geqq n)$ is any simple variety on V, defined over a field $k' \supset k$ which is free with respect to K over k, then*

- **i.** *for a point Q which is generic on U over K' (the composition of K and k') we have that $W \cdot (Q \times V) = Q \times W(Q)$, where $W(Q) = A^*$ is a $K(Q)$-prime rational cycle with reduced expression $A^* = \sum_\mu A^*_\mu$ (i.e., with coefficients 1), which is such that $A^* \cdot B = \sum_i C_i$ with $C_i \neq C_j$ for $i \neq j$ and $\sum_i C_i$ is $K'(Q)$-prime rational. (This remains true if B is a k'-prime rational cycle with reduced expression $B = \sum_i B_i$). Furthermore, a generic point of C_i over a field of definition for C_i is generic on B over k'.*
- **ii.** *$W \cdot (Q' \times V) = Q' \times (A + \sum_\lambda \eta_\lambda A_\lambda)$, where A_λ is such that*
  - **a.** *every component C of $A_\lambda \cap B$, which is not contained in $A \cap B$, is a proper component of $A_\lambda \cap B$ on V, and a generic point of C over a field of definition for C is generic on B over k.*
  - **b.** *if D is a simple subvariety of V defined over a field which contains k and which is free with respect to K over k, then there is always a point of D outside all the A_λ.*

Furthermore, this system U, W, K, and Q' can always be selected in such a way that K is free with respect to an arbitrary given extension field of k.

(Notes: 1. It follows in particular from **iib.** that every component of $A_\lambda \cap B$,

---

** Cf. also Lemma 2, page 456, of W. L. Chow, "On equivalence classes of cycles in an algebraic variety," *Annals of Mathematics*, vol. 64 (1956), pp. 450-479.

which is contained in a simple component of $A \cap B$, is contained strictly in that component.

2. If $A \cdot B$ is defined, then all the $A_\lambda \cdot B$ are defined.
3. In the following, we often denote such a system U, W, K and Q' by $[U, W, K, Q'; A, V, k]$.)

Proof. Let V^n be in P^N, let L^{N-n-1} be a linear space generic over k. For K, we take the algebraic closure of the smallest field of definition for L containing k. For U, we take P^{N^2+2N}; every point of U can be interpreted as an $(N+1)$-square matrix to which belongs a projective transformation of P^N, and, conversely, to every $(N+1)$-square matrix belongs a point of U. Let Q' be the point belonging to the identity matrix. For W we take the locus over K of the point (T, P), here T is a generic point on U over K and P is a generic point over $K(T)$ of the $K(T)$-prime rational cycle $V \cdot \Gamma^T$ (see Lemma 2), where $\Gamma = \Gamma_{(A,L)}$.

We have to show that U, W, K and Q' fulfill the requirements. Consider $W(Q)$ for Q generic over K on U; the V-cycle $W(Q)$ considered as a P^N-cycle is equal, by construction, to $\Gamma^Q \cdot V$. By Lemma 2, applied to Γ and V, the cycle $W(Q)$ is $K(Q)$-prime rational and has the required expression. If B^b is any simple subvariety of V, defined over a field k' (as described in the proposition, and if Q is generic over K'), then $W(Q) \cap B$ is, as a point-set, the same as $\Gamma^Q \cap B$; hence, by Lemma 1i. and **ii.**, every component of $W(Q) \cap B$ is proper and simple on V. Let C_i be such a component, then C_i is also a component of $\Gamma^Q \cap B$. Now if $W(Q) = A^* = \sum_\mu A^*_\mu$, then by [VI], Chap. VI, Th. 9, and since $\boldsymbol{i}(\Gamma^Q \cdot V, A^*_\mu; P^N) = 1$ by Lemma 1**i.**, we have

$$\begin{aligned} \boldsymbol{i}(W(Q) \cdot B, C_i; V) &= \textstyle\sum_\mu \boldsymbol{i}(A^*_\mu \cdot B, C_i; V) \\ &= \textstyle\sum_\mu \boldsymbol{i}(A^*_\mu \cdot B, C_i; V)\, \boldsymbol{i}(\Gamma^Q \cdot V, A^*_\mu; P^N) = \boldsymbol{i}(\Gamma^Q \cdot B, C_i; P^N) = 1. \end{aligned}$$

Therefore the V-cycle $A^* \cdot B = \sum_i C_i$, if considered as a cycle in P^N, is equal to $\Gamma^Q \cdot B$; from this, all the remaining assertions of **i.** follow by Lemma 2. The same reasoning holds if B is a k'-prime rational cycle and equal to $\sum_i B_i$.

Consider the locus W_1 of (T, R) over K, where, as before T is generic on U over K, and where R is generic over $K(T)$ on Γ^T. (Note that $W_1 \cdot (Q' \times P^N) = Q' \times \Gamma$, as follows by considering a system of equations for W_1.) Next we show that W is a proper component of multiplicity 1 of $W_1 \cap (U \times V)$ and that every other component of that intersection has on U a projection smaller than U. Clearly $W \subset W_1 \cap (U \times V)$. Let Y be a component of $W_1 \cap (U \times V)$ with projection U on U. Consider $Y \cap (T \times P^N)$ for T generic over K on U; by assumption, this is not empty. Let $T \times R'$

be a generic point over the algebraic closure of $K(T)$ of a component $T \times Z$ of $Y \cap (T \times P^N)$; by [VI], Chap. VI, Th. 11, $T \times R'$ is generic on Y over K. We have

$$T \times Z \subset Y \cap (T \times P^N) \subset W_1 \cap (U \times V) \cap (T \times P^N)$$
$$= (T \times \Gamma^T) \cap (U \times V) \subset T \times (V \cap \Gamma^T).$$

Hence $T \times R'$ is on W and $Y = W$ for dimension reasons. Since

$$\boldsymbol{i}(\Gamma^T \cdot V, C_i; P^N) = 1$$

by Lemma 1**i.**, it follows by [VI], Chap. VI, Th. 7 that

$$\boldsymbol{i}[(T \times \Gamma^T) \cdot (U \times V), T \times C_i; U \times P^N] \cdot \boldsymbol{i}[W_1 \cdot (T \times P^N), T \times \Gamma^T; U \times P^N] = 1$$

(the second factor is 1 by [VI], Chap. VI, Th. 11). Therefore, by the associativity of the $\boldsymbol{i}$-symbol ([VI], Chap. VI, Th. 5),

$$\boldsymbol{i}[W_1 \cdot (U \times V), W; U \times P^N] \cdot \boldsymbol{i}[W \cdot (T \times P^N)), T \times C_i; U \times P^N] = 1.$$

Hence $\boldsymbol{i}[W_1 \cdot (U \times V), W; U \times P^N] = 1$.

Consider next the point Q'. If Y is any component of $W_1 \cap (U \times V)$, different from W, then $Y\{Q'\}$ either is empty or consists entirely of singular points on V. For, by [VI], Chap. VI, Cor. 1 of Th. 1, dim. $Y \geqq N^2 + 2N + a$; since the projection of Y on U is, as we have seen, smaller then U, it follows (again by the same corollary[2]) that if there is a simple point in $Y\{Q'\}$, then $Y\{Q'\}$ must have a component of dimension greater than a. However, $Y\{Q'\} \subset V \cap \Gamma$, for

$$Q' \times Y\{Q'\} = Y \cap (Q' \times V) \subset W_1 \cap (U \times V) \cap (Q' \times P^N)$$
$$= (Q' \times \Gamma) \cap (U \times V);$$

hence $Y\{Q'\}$ has only components of dimension $\leqq a$ by Lemma 3**i.** Since every component of $W_1(Q') \cap V = \Gamma \cap V$ is simple on V by Lemma 3**i.**, it follows that the components of $W_1(Q') \cap V$ are the same as the components of $W\{Q'\}$. Hence, for dimension reasons, $W(Q')$ is defined, and if $V \cap W_1(Q') = A + \sum_\lambda \eta'_\lambda A_\lambda$ (see Lemma 3**i.**), then $W(Q') = \eta A + \sum_\lambda \eta_\lambda A_\lambda$.

---

[2] Apparently, there arises a difficulty if we want to apply [VI], Chap. VI, Cor. 1 of Th. 1 in the above mentioned situation. For if Y' is the projection on U of Y, then we have to consider the intersection $Y \cap (Q' \times V)$ on $Y' \times V$; however, it could be that Q' is singular on Y'. Therefore we apply the corollary to the following situation: Let X be a curve on U, going through Q' and such that a generic point of X over a field of definition for X is generic on U over K. Let the simple point in $Y\{Q'\}$ be denoted by S. Apply the above mentioned corollary to $Y \cap (X \times V)$; it follows that there is a component Z, containing $Q' \times S$, which is at least of dimension $a + 1$. Since $\mathrm{pr}_U Z \subset X$ and $\mathrm{pr}_U Z \neq X$ (for X contains a generic point of U over K and $\mathrm{pr}_U Z \subset \mathrm{pr}_U Y \neq U$), it follows that $Z \subset Y\{Q'\}$.

Using the fact that $\boldsymbol{i}[W_1\cdot(U\times V), W; U\times P^N]=1$, the associativity of the $\boldsymbol{i}$-symbol ([VI], Chap. VI, Th. 5) and some trivialities, we obtain

$$\begin{aligned}\eta&=\boldsymbol{i}[W\cdot(Q'\times V), Q'\times A; U\times V]=\boldsymbol{i}[W\cdot(Q'\times P^N), Q'\times A; U\times P^N]\\&=\boldsymbol{i}[W\cdot(Q'\times P^N), Q'\times A; U\times P^N]\cdot\boldsymbol{i}[W_1\cdot(U\times V), W; U\times P^N]\\&=\boldsymbol{i}[W_1\cdot(Q'\times P^N), Q'\times\Gamma; U\times P^N]\boldsymbol{i}[(Q'\times\Gamma)\cdot(U\times V),\\&\qquad Q'\times A; U\times P^N]=\boldsymbol{i}(\Gamma\cdot V, A; P^N)=1.\end{aligned}$$

All the remaining assertions follow from Lemma 3**ii.** and **iii.** This completes the proof.

2. Definition of the $\boldsymbol{i}$-symbol and some of its properties. First we introduce some concepts and notations which are frequently used in the following. If $\sum_i n_i R_i$ is a 0-dim. cycle on a variety V, and if $\mathscr{B}$ is a bunch on V, then we understand by " the number of points of $\sum_i n_i R_i$ which are in $\mathscr{B}$" the number of points R_i which are in $\{\mathscr{B}\}$, each counted with the integer n_i.[3] If $\mathscr{B}$ and $\mathfrak{D}$ are bunches on V, such that every component C of $\mathscr{B}$ is *strictly* contained in a component D of $\mathfrak{D}$, then we shall say that $\mathscr{B}$ is strictly contained component-wise in $\mathfrak{D}$, and we write $\mathscr{B}\prec\mathfrak{D}$ or $\mathfrak{D}\succ\mathscr{B}$.

Let A^a and B^b be subvarieties of a projective variety V^n. Let $\mathscr{B}$ be a maximal connected bunch of $A\cap B$, and assume that every point of $\{\mathscr{B}\}$ is simple on V. If C is a component of $\mathscr{B}$, i.e., a component of $A\cap B$, then we define the *excess* of C as a component of the intersection of A and B on V as the integer $\dim. C-a-b+n$; the maximum of these integers over all the components of $\mathscr{B}$ we call the *excess of* $\mathscr{B}$ as a maximal connected bunch of $A\cap B$ on V.

From now on, we assume $a+b=n$. We want to define an integer $\boldsymbol{i}(A\cap B, \mathscr{B}; V)$, called the *intersection multiplicity of A and B on V at $\mathscr{B}$*. By induction on the excess of $\mathscr{B}$, we assume that such an integer is defined and that the symbol is commutative (i.e., $\boldsymbol{i}(A\cap B,\mathscr{B};V)=\boldsymbol{i}(B\cap A,\mathscr{B};V)$) if the excess of $\mathscr{B}$ is smaller than some integer d. (For excess $\mathscr{B}=0$ there is such a multiplicity theory in [VI], Chap. VI.) Now let $\mathscr{B}$ be a maximal connected bunch of $A\cap B$, with excess equal to d.

Let k be a field of definition for A, B and V. Let (with respect to the varieties A and V and the field k) the varieties U and W, the field K and the point P' have the properties mentioned in Proposition 1. For convenience of notation, we shall denote this system by $\alpha=[U, W, K, P'; A, V, k]$. Let P be a generic point on U over K; writing, as in Proposition 1, $W(P)=A^*$, we have, by our assumptions on the system α, $A^*\cdot B=\sum_i R_i$ with $R_i\neq R_j$ for

---

[3] $\{\mathscr{B}\}$ denotes the point-set attached to $\mathscr{B}$. (Cf. [VI], page 84).

$i \neq j$ and $\sum_i R_i$ *prime* rational over $K(P)$ (here $k' = k$, hence $K' = K$). Let $\mathcal{D}_{\lambda i}$ be those maximal connected bunches of $A_\lambda \cap B$ which are in $\{\mathscr{B}\}$; by our assumptions on the system α, these are the only bunches of $A_\lambda \cap B$ which have points in common with $\{\mathscr{B}\}$, and we have $\mathcal{D}_{\lambda i} \prec \mathscr{B}$ for all couples λ, i (see Prop. 1**iia.** and **iib.**). By the induction assumption, $\boldsymbol{i}(A_\lambda \cap B, \mathcal{D}_{\lambda i}; V)$ is defined. Let $\sum_i R'_i$ be a specialization of $\sum_i R_i$ over the specialization $P \rightarrow P'$ with reference to K.[3a] (Note that, by the specialization theorem, [III], page 104, A^* specializes uniquely to $A + \sum_\lambda \eta_\lambda A_\lambda$ over the specialization $P \rightarrow P'$ with reference to K). Let σ be the number of points of $\sum_i R'_i$ which are in $\{\mathscr{B}\}$. Our first purpose is to show that σ is independent of the particular specialization $\sum_i R'_i$ of $\sum_i R_i$ over the specialization $P \rightarrow P'$ with reference to K. Consider the locus G over K of the point (P, R_i). Since $\sum_i R_i$ is $K(P)$-prime rational, this is independent of i; G is a subvariety of $U \times V$. Consider the total transform of the point P' (which, by assumption, is simple on U) by G. Since $R_i \in A^* \cap B$, it follows that the maximal connected bunches of $G\{P'\}$ are contained in the maximal connected bunches of $A \cap B$ and $A_\lambda \cap B$ (by [III], page 53g since $A^* \rightarrow A + \sum_\lambda \eta_\lambda A_\lambda$ and $B \rightarrow B$ if $P \rightarrow P'$ with reference to K); by our previous remarks, those bunches are either entirely inside or entirely outside $\{\mathscr{B}\}$. Apply [II], Th. 3 to those maximal connected bunches of $G\{P'\}$ which are contained in $\{\mathscr{B}\}$; it follows that σ is independent of the particular specialization $\sum_i R'_i$ of $\sum_i R_i$ over the specialization $P \rightarrow P'$ with reference to K.

Define

$$(1) \qquad \boldsymbol{i}_\alpha(A \cap B, \mathscr{B}; V) = \sigma - \textstyle\sum_\lambda \eta_\lambda \sum_i \boldsymbol{i}(A_\lambda \cap B, \mathcal{D}_{\lambda i}; V).^4$$

First of all we shall show that if $\{\mathscr{B}\}$ is reduced to a point C (and hence $\boldsymbol{i}_\alpha(A \cap B, \mathscr{B}; V) = \sigma$), then $\boldsymbol{i}_\alpha(A \cap B, \mathscr{B}; V) = \boldsymbol{i}(A \cdot B, C; V)$. Consider again the variety G introduced above. By [VI], Chap. VI, Th. 12, it follows that $\sigma = \boldsymbol{i}[G \cdot (P' \times V), P' \times C; U \times V]$. Clearly G is a component of $(U \times B) \cap W$, and it is the only component with projection U on U. For dimension reasons, it is a proper component on $U \times V$; moreover, it is a proper component of multiplicity 1 as follows from the computation (if $R_i \in A^*_\mu$)

$$\begin{aligned} 1 &= \boldsymbol{i}(A^*_\mu \cdot B, R_i; V) = \boldsymbol{i}[(P \times A^*_\mu) \cdot (U \times B), P \times R_i; U \times V] \\ &= \boldsymbol{i}[(P \times V) \cdot W, P \times A^*_\mu; U \times V]\boldsymbol{i}[(P \times A^*_\mu) \cdot (U \times B), P \times R_i; U \times V] \\ &= \boldsymbol{i}[W \cdot (U \times B), G; U \times V]\boldsymbol{i}[(P \times V) \cdot G, P \times R_i; U \times V] \end{aligned}$$

[3a] Specializations of (positive) cycles on V have to be understood as follows: take a specialization of the cycle in projective space and omit in the summation all components which are singular on V. (Cf. W. L. Chow, loc. cit. in **.)

[4] This integer can be negative; see footnote 11 in [V], page 639.

by (except for some trivialities) the associativity of the $\boldsymbol{i}$-symbol, [VI], Chap. VI, Th. 5. Moreover, there is no component G' of $(U \times B) \cap W$ which contains $P' \times C$. For if G' should be such a component, then the projection of G' on U is smaller than U; hence, by [VI], Chap. VI, Cor. 1 of Th. 1, every component D of $G'\{P'\}$ containing $P' \times C$ is of dimension greater than zero.[5] However, $D \subset A \cap B$, for

$$\begin{aligned} G' \cap (P' \times V) &\subset (U \times B) \cap W \cap (P' \times V) \\ &\subset [(U \times B) \cap (P' \times A)] \cup [\bigcup_{\lambda} (U \times B) \cap (P' \times A_{\lambda})] \\ &\subset P' \times (A \cap B) \cup [\bigcup_{\lambda} A_{\lambda} \cap B]. \end{aligned}$$

Hence, since for all λ, $C \not\subset A_{\lambda}$ (Prop. **1iib.**), it follows that $D \subset A \cap B$; but then C is not a component of $A \cap B$ since it is contained in the component D. Therefore, we have that

$$\begin{aligned} \sigma &= \boldsymbol{i}[G \cdot (P' \times V), P' \times C; U \times V] \\ &= \boldsymbol{i}[G \cdot (P' \times V), P' \times C; U \times V]\boldsymbol{i}[W \cdot (U \times B), (U \times B), G; U \times V] \\ &= \boldsymbol{i}[(P' \times V) \cdot W, P' \times A; U \times V]\boldsymbol{i}[(P' \times A) \cdot (U \times B), P' \times C; U \times V] \end{aligned}$$

(by [VI], Chap. VI, Th. 5). Since the first factor of the last product is 1 (see Prop. **1ii**), it follows that $\sigma = \boldsymbol{i}[(P' \times A) \cdot (U \times B), P' \times C; U \times V] = \boldsymbol{i}(A \cdot B, C; V)$ by [VI], Chap. VI, Th. 7.

Next we want to show that $\boldsymbol{i}_{\alpha}(A \cap B, \mathscr{G}; V)$ is, in fact, independent of the system $\alpha = [U, W, K, P'; A, V, k]$. Consider a system $\beta = [X, Y, K_1, Q'; B, V, k]$ having the properties of Proposition 1, and let K_1 be free with respect to $K(P)$ over k; let the compositum of K and K_1 *be* K_2. We have $Y \cdot (Q' \times V) = Q' \times (B + \sum_{\mu} \pi_{\mu} B_{\mu})$. Let those maximal connected buches of $A \cap B_{\mu}$ which are in $\{\mathscr{G}\}$ be denoted by $\mathcal{E}_{\mu j}$, and let those maximal connected bunches of $A_{\lambda} \cap B_{\lambda}$ which are in $\{\mathscr{G}\}$ be denoted by $\mathcal{F}_{\lambda\mu h}$. (By the assumptions on the system β, and since A and A_{λ} are defined over a field K which is free with respect to K_1 over k, it follows by Prop. **1iib.** that $\mathcal{E}_{\mu j} \prec \mathscr{G}$ and for a fixed λ, μ and h there is an index i such that $\mathcal{F}_{\lambda\mu h} \prec \mathcal{D}_{\lambda i}$;[6] similarly, by the assumptions on the system α, and since the B_{μ} are defined over K_1, which is free with respect to K over k, it follows that for a fixed λ, μ and h there is an index j such that $\mathfrak{J}_{\lambda\mu h} \prec \mathcal{E}_{\mu j}$. Furthermore, we note that these bunches are the only maximal connected bunches of the intersections under consideration which have points in common with $\{\mathscr{B}\}$.) By our induction assumption on the commutativity of the i-symbol, we have

---

[5] We have to use here the same kind of argument as in footnote 2.

[6] The variety A_{λ} is defined over the field K which is free with respect to K_1 over k, and the system β has the properties of Proposition 1. Therefore, it follows by Prop. 1iia. and iib. that a component G of $A_{\lambda} \cap B_{\mu}$ which has points in common with $\{\mathscr{G}\}$ either is contained strictly in a component of $A_{\lambda} \cap B$ (which then must have points in common with $\{\mathscr{G}\}$, i. e., which must be in a $\mathfrak{D}_{\lambda i}$) or is proper. In the latter case, this component G is a point, generic on A_{λ} over K; however this is impossible since $G \in \{\mathscr{G}\}$, and hence A_{λ} should be contained in A.

$$\boldsymbol{i}(A_\lambda \cap B_\mu, \mathfrak{J}_{\lambda\mu h}; V) = \boldsymbol{i}(B_\mu \cap A_\lambda, \mathfrak{J}_{\lambda\mu h}; V).$$

Let Q be a generic point of X over $K_2(P)$. By the properties of the system β, we have that the following cycles are defined: $A^* \cdot B^* = \sum_i S_i$, $A \cdot B^* = \sum_i T_i$ and $A_\lambda \cdot B^* = \sum_i T_{\lambda i}$; furthermore, $S_i \neq S_j$, $T_i \neq T_j$, $T_{\lambda i} \neq T_{\lambda j}$ and $\sum_i S_i$, $\sum_i T_i$ and $\sum_i T_{\lambda i}$ are prime rational over $K_2(P, Q)$, $K_2(Q)$ and $K_2(Q)$ respectively. Similarly, by the properties of the system α, we have [except $A^* \cdot B = \sum_i R_i$, $R_i \neq R_j$ and $\sum_i R_i$ prime rational over $K_2(P)$] also that $A^* \cdot B_\mu = \sum_i R_{\mu i}$ with $R_{\mu i} \neq R_{\mu j}$ and $\sum_i R_{\mu i}$ prime rational over $K_2(P)$.

Next consider a specialization $(Q, \sum_i T_i) \rightarrow (Q', \sum_i T'_i)$ over K_1 (hence, by [VI], Chap. II, Th. 4, a fortiori over K_2 since K_2 is the compositum of K and K_1 and K is free with respect to (Q) over K_1). Let τ be the number of points of $\sum_i T'_i$ *which are in* $\{\mathscr{B}\}$; then by definition

$$(2) \qquad \boldsymbol{i}_\beta(B \cap A, \mathscr{B}; V) = \tau - \textstyle\sum_\mu \pi_\mu \sum_j \boldsymbol{i}(B_\mu \cap A, \mathcal{E}_{\mu j}; V).$$

We intend to show that $\boldsymbol{i}_\alpha(A \cap B, \mathscr{B}; V) = \boldsymbol{i}_\beta(B \cap A, \mathscr{B}; V)$.

Let E be the locus of (P, Q, S_i) over K_2; since $S_i \in A^* \cap B^*$ and since A^* and B^* specialize to $A + \sum_\lambda \eta_\lambda A_\lambda$ and $B + \sum_\mu \pi_\mu B_\mu$ if $P \rightarrow P'$ and $Q \rightarrow Q'$ over K_2, it follows (by [III], page 53g) that the maximal connected bunches of $E\{P', Q'\}$ are contained in the maximal connected bunches of $A \cap B$, $A \cap B_\mu$, $A_\lambda \cap B$ and $A_\lambda \cap B_\mu$. By what is shown above about the bunches of those intersections, it follows that the maximal connected bunches of $E\{P', Q'\}$ are either entirely inside or entirely outside $\{\mathscr{B}\}$. Apply [II], Th. 3 to $E \subset U \times X \times V$, to the simple point (P', Q') of $U \times X$ and to those maximal connected bunches of $E\{P', Q'\}$ which are in $\{\mathscr{B}\}$. It follows that the number of points of every specialized cycle of $\sum_i S_i$, over the specialization $(P, Q) \rightarrow (P', Q')$ with reference to K_2, which are in $\{\mathscr{B}\}$ is always the same. Consider, in particular, the specialization

$$(P, Q, \textstyle\sum_i S_i) \rightarrow (P, Q', A^* \cdot [B + \sum_\mu \pi_\mu B_\mu])$$
$$\rightarrow (P', Q', \textstyle\sum_i S'_i = \sum_i R'_i + \sum_\mu \pi_\mu \sum_i R'_{\mu i})$$

over K_2 [it is easily seen by [VI], Chap. II, Th. 4 that $(P, A^* \cdot B) \rightarrow (P', \sum_i R'_i)$ not only over K but also over K_2]; let n', σ and σ_μ be, respectively, the number of points of $\sum_i S'_i$, of $\sum_i R'_i$ and of $\sum_i R'_{\mu i}$ which are in $\{\mathscr{B}\}$ [σ has been introduced above]. Clearly $n' = \sigma + \sum_\mu \pi_\mu \sigma_\mu$. On the other hand, consider the specialization

$$(P, Q, \textstyle\sum_i S_i) \rightarrow (P', Q, [A + \sum_\lambda \eta_\lambda A_\lambda] \cdot B^*)$$
$$\rightarrow (P', Q', \textstyle\sum_i S''_i = \sum_i T'_i + \sum_\lambda \eta_\lambda \sum_i T'_{\lambda i})$$

over K_2; let n'', τ and τ_λ be the number of points of $\sum_i S''_i$, of $\sum_i T'_i$ and of $\sum_i T'_{\lambda i}$ which are in $\{\mathcal{B}\}$. Clearly $n'' = \tau + \sum_\lambda \eta_\lambda \tau_\lambda$. As we have just seen, $n' = n''$. Hence

$$\sigma + \textstyle\sum_\mu \pi_\mu \sigma_\mu = n' = n'' = \tau + \sum_\lambda \eta_\lambda \tau_\lambda. \tag{3}$$

By the definition of the $\boldsymbol{i}$-symbol, we have (if we make use of the above mentioned relations between the $\mathcal{D}_{\lambda i}$, the $\mathcal{E}_{\mu j}$ and the $\mathcal{F}_{\lambda\mu h}$) after a summation:

$$\begin{aligned}\textstyle\sum_\mu \pi_\mu \sum_j \boldsymbol{i}(A \cap B_\mu, \mathcal{E}_{\mu j}; V) \\ = \textstyle\sum_\mu \pi_\mu \sigma_\mu - \sum_\mu \pi_\mu \sum_{\lambda, h} \eta_\lambda \boldsymbol{i}(A_\lambda \cap B_\mu, \mathcal{F}_{\lambda\mu h}; V)\end{aligned} \tag{4}$$

and

$$\begin{aligned}\textstyle\sum_\lambda \eta_\lambda \sum_i \boldsymbol{i}(B \cap A_\lambda, \mathcal{D}_{\lambda i}; V) \\ = \textstyle\sum_\lambda \eta_\lambda \tau_\lambda - \sum_\lambda \eta_\lambda \sum_{\mu, h} \pi_\mu \boldsymbol{i}(B_\mu \cap A_\lambda, \mathcal{F}_{\lambda\mu h}; V).\end{aligned} \tag{5}$$

(The equations (4) and (5) are essentially nothing else but the definitions of $\boldsymbol{i}(A \cap B_\mu, \mathcal{E}_{\mu j}; V)$ and $\boldsymbol{i}(B \cap A_\lambda, \mathcal{D}_{\lambda i}; V)$ respectively.) In view of the commutativity of the $\boldsymbol{i}$-symbols (induction assumption), the last sums in (4) and (5) are equal. From this, one obtains from (4), (5) and (3) that

$$\sigma + \textstyle\sum_\mu \pi_\mu \sum_j \boldsymbol{i}(A \cap B_\mu, \mathcal{E}_{\mu j}; V) = \tau + \sum_\lambda \eta_\lambda \sum_i \boldsymbol{i}(B \cap A_\lambda, \mathcal{D}_{\lambda i}; V).$$

From this, again after having used the commutativity of the $\boldsymbol{i}$-symbol for the bunches $\mathcal{D}_{\lambda i}$ and $\mathcal{E}_{\mu j}$ which have an excess smaller than excess $\mathcal{B}$, it follows from the definitions (1) and (2) that $\boldsymbol{i}_\alpha(A \cap B, \mathcal{B}; V) = \boldsymbol{i}_\beta(B \cap A, \mathcal{B}; V)$.

From the fact that $\boldsymbol{i}_\beta$ is independent of the system α, it follows first that $\boldsymbol{i}_\alpha(A \cap B, \mathcal{B}; V)$ is independent of α; therefore we can write $\boldsymbol{i}(A \cap B, \mathcal{B}; V)$, and next we can conclude from our result $\boldsymbol{i}_\alpha(A \cap B, \mathcal{B}; V) = \boldsymbol{i}_\beta(B \cap A, \mathcal{B}; V)$ the commutativity of the $\boldsymbol{i}$-symbol.

THEOREM 1. *Let A^a and B^b be subvarieties of a projective variety V^n $(n = a + b)$. Let $\mathcal{B}$ be a maximal connected bunch of $A \cap B$ on V, such that every point of $\{\mathcal{B}\}$ is simple on V. Then $\boldsymbol{i}(A \cap B, \mathcal{B}; V) = \boldsymbol{i}(B \cap A, \mathcal{B}; V)$.*

Another immediate consequence of the definition is the *birational invariance* of the $\boldsymbol{i}$-symbol for birational transformations which are biregular at every point of $\{\mathcal{B}\}$.

THEOREM 2. *Let A^a and B^b be subvarieties of a projective variety V^n $(n = a + b)$. Let $\mathcal{B}$ be a maximal connected bunch of $A \cap B$, such that* *every point of* $\{\mathfrak{B}\}$ *is simple on* V. *Let* T *be a birational correspondence between* V *and a projective variety* V', *biregular at every point of* $\{\mathfrak{B}\}$. *Let* A', B' *and* $\mathfrak{B}'$ *correspond with* A, B *and* $\mathfrak{B}$ *by* T. *Then* $\mathfrak{B}'$ *is a maximal connected bunch of* $A' \cap B'$ *and* $\boldsymbol{i}(A \cap B, \mathfrak{B}; V) = \boldsymbol{i}(A' \cap B', \mathfrak{B}'; V')$.

Proof. By induction on the excess of $\mathfrak{B}$. Let the notations be as above. We observe that, from the fact that T is biregular at every point of $\{\mathfrak{B}\}$, it follows that T is biregular at every point R_i of $A^* \cdot B$ and at every A_λ (a generic point of A_λ over K is, namely, generic on V over k, as follows from Prop. 1**iia.**). From this, one concludes by standard reasoning that every integer in (1) is equal to the corresponding integer with primes; hence $\boldsymbol{i}(A \cap B, \mathfrak{B}; V) = \boldsymbol{i}(A' \cap B', \mathfrak{B}'; V')$.

3. Some further properties of the $\boldsymbol{i}$-symbol.

THEOREM 3. *Let* B^b *be a simple subvariety of a projective variety* V^n. *Let* $\mathfrak{B}$ *be a bunch of subvarieties of* V *such that every point of* $\{\mathfrak{B}\}$ *is simple on* V. *Suppose there is a variety* U *and a subvariety* W *of* $U \times V$ *with the following properties:*

i. *If* Q *is a generic point on* U *over a common field of definition* k *for* B, V, U *and* W, *then the cycle* $W(Q) = A^*$ *is defined, is of dimension* $n - b$, *and is such that every component of* $W(Q) \cap B$ *is a point if this component is simple on* V. *Let* $A^* \cdot B = \sum_i R_i$ *(it is not excluded that* $R_i = R_j$ *for* $i \neq j$*).*

ii. *There is a point* Q', *simple on* U, *such that the cycle* $W(Q')$ *is defined and* $W(Q')$ *is such that the maximal connected bunches of* $W(Q') \cap B$ *are either entirely contained in* $\{\mathfrak{B}\}$ *or do not have any point in common with* $\{\mathfrak{B}\}$. *Let* $W(Q') = \sum_\lambda \eta_\lambda A_\lambda$ *(reduced expression), and let* $\mathfrak{B}_{\lambda i}$ *be those maximal connected bunches of* $A_\lambda \cap B$ *which are in* $\{\mathfrak{B}\}$.

Suppose $\sum_i R'_i$ *is a specialization of* $\sum_i R_i$ *over the specialization* $Q \to Q'$ *with reference to* k, *let* σ *be the number of points of* $\sum_i R'_i$ *which are in* $\{\mathfrak{B}\}$. *Then* $\sigma = \sum_\lambda \eta_\lambda \sum_i \boldsymbol{i}(A_\lambda \cap B, \mathfrak{B}_{\lambda i}; V)$.

Proof. We proceed by induction on the integer $\max._{C \in \mathfrak{C}} \dim. C$; let this integer be denoted by d. The proof for the case $d = 0$ is included in the considerations below. Furthermore, for convenience, we assume that k is such that Q' is rational in k. Write $A^* = \sum_\gamma \alpha_\gamma A^*_\gamma$ with A^*_γ $k(Q)$-prime rational; let $A^*_\gamma \cdot B = \sum_i R_{\gamma i}$, hence $\sum_\gamma \alpha_\gamma \sum_i R_{\gamma i} = \sum_i R_i$. Let

$$\beta = [X, Y, K, P'; B, V, k]$$

be a system having the properties of Proposition 1, where K is free with respect to $k(Q)$ over k. Write $B^* = Y(P)$ for P generic on X over $K(Q)$. By assumption on the system β, we have $A^* \cdot B^* = \sum_\gamma \alpha_\gamma A^*_\gamma \cdot B^* = \sum_\gamma \alpha_\gamma \sum_i S_{\gamma i}$ with $S_{\gamma i} \neq S_{\gamma j}$ and $\sum_i S_{\gamma i}$ is $K(Q, P)$-prime rational. Let $Y(P') = B + \sum \pi_\mu B_\mu$. It follows by the properties of the system β (see Prop. 1**iii.**) that all the $A^* \cdot B_\mu$ are defined (since $A^* \cdot B$ is defined); write $A^* \cdot B_\mu = \sum_{\mu, i} R_{\mu i}$. Let $\mathcal{D}_{\lambda\mu j}$ be those maximal connected bunches of the $A_\lambda \cap B_\mu$ which have points in common with $\{\mathcal{B}\}$. It follows by the properties of the system β (see Prop. 1**ii.**) that for every $\mathcal{D}_{\lambda\mu j}$, either there is a $\mathcal{B}_{\lambda i}$ such that $\mathcal{D}_{\lambda\mu j} \prec \mathcal{B}_{\lambda i}$ or $\mathcal{D}_{\lambda\mu j}$ is reduced to a point and hence is a proper component of $A_\lambda \cap B_\mu$ on V.

Let E_γ be the locus of $(P, Q, S_{\gamma i})$ over K (E_γ is independent of the index i since $\sum_i S_{\gamma i}$ is $K(P, Q)$-prime rational); $E_\gamma \subset U \times X \times V$. The maximal connected bunches of $E_\gamma\{P', Q'\}$ are contained in maximally connected unions of the maximal connected bunches of the $A_\lambda \cap B$ and the $A_\lambda \cap B_\mu$; therefore—as explained above—the maximal connected bunches of $E_\gamma\{P', Q'\}$ are either entirely inside or entirely outside $\{\mathcal{B}\}$. Apply [II], Th. 3 to every variety E_γ and to those maximal connected bunches of $E_\gamma\{P', Q'\}$ which are in $\{\mathcal{B}\}$; since (P', Q') is simple on $U \times X$, it follows that the number of points which are in $\{\mathcal{B}\}$ of a specialization of the cycle $\sum_i S_i$ over the specialization $(P, Q) \rightarrow (P', Q')$, with reference to K, is always the same, independent of the specialization ($\sum_i S_i = A^* \cdot B^*$). Consider first the specialization

$$\begin{aligned}(P, Q, \textstyle\sum_i S_i) &\rightarrow (P', Q, A^* \cdot [B + \textstyle\sum_\mu \pi_\mu B_\mu]) \\ &\rightarrow (P', Q', \textstyle\sum_i S'_i = \sum_i R'_i + \sum_{\mu, i} \pi_\mu R'_{\mu i})\end{aligned}$$

over K; let n', σ and σ_μ be, respectively, the number of points of $\sum_i S'_i$, of $\sum_i R'_i$ and of $\sum_i R'_{\mu i}$ which are in $\{\mathcal{B}\}$. Next, consider the specialization $(P, Q, \sum_i S_i) \rightarrow (P, Q', [\sum_\lambda \eta_\lambda A_\lambda] \cdot B^*) \rightarrow (P', Q', \sum_i S''_i = \sum_{\lambda, i} \eta_\lambda T'_{\lambda i})$ over K (with obvious notations); let n'' and τ_λ be the number of points of $\sum_i S''_i$ and $\sum_i T'_{\lambda i}$ respectively, which are in $\{\mathcal{B}\}$. We have seen $n' = n''$; hence

$$\sigma + \textstyle\sum_\mu \pi_\mu \sigma_\mu = n' = n'' = \sum_\lambda \eta_\lambda \tau_\lambda. \tag{1}$$

Since—as we have seen above—every $\mathcal{D}_{\lambda\mu j}$ either is strictly contained componentwise in a certain $\mathcal{B}_{\lambda i}$ or is a proper component of intersection, we can apply, by our induction assumption, the theorem to every variety B_μ, to the bunches $\mathcal{D}_{\lambda\mu j}$ (μ fixed), and to the cycle $A^* \cdot B_\mu$ and its specialization $\sum_i R'_{\mu i}$ over the specialization $Q \rightarrow Q'$ with reference to K. This gives

$$\sigma_\mu = \textstyle\sum_\lambda \eta_\lambda \sum_j \boldsymbol{i}(A_\lambda \cap B_\mu, \mathcal{D}_{\lambda\mu j}; V). \tag{2}$$

(If the integer d, introduced in the beginning, is zero, then there are no bunches $\mathscr{D}_{\lambda\mu j}$, as follows from Prop. **1iib.** applied to the system β). Next we use the definitions of the symbols $\boldsymbol{i}(B \cap A_\lambda, \mathscr{B}_{\lambda i}; V)$. A summation over all the bunches $\mathscr{B}_{\lambda i}$ (λ fixed) gives

$$(3) \qquad \tau_\lambda = \textstyle\sum_i \boldsymbol{i}(B \cap A_\lambda, \mathscr{B}_{\lambda i}; V) + \sum_\mu \pi_\mu \sum_j \boldsymbol{i}(B_\mu \cap A_\lambda, \mathscr{D}_{\lambda\mu j}; V).$$

By (1), (2), (3) and the commutativity of the $\boldsymbol{i}$-symbol, the required formula follows immediately.

THEOREM 4 (Projection theorem). *Let B^b be a subvariety of $U^n \times V^m$, where U and V are projective varieties. Let B_1 be the projection of B on U and let* dim. $B =$ dim. B_1. *Let A^a $(a + b = n)$ be a subvariety of U. Let $\mathscr{B}$ be a maximal connected bunch of $A \cap B_1$, and let $\mathscr{B}_\gamma$ be those maximal connected bunches of $(A \times V) \cap B$ which project (as point-sets) into $\{\mathscr{B}\}$. Assume that all the points of $\{\mathscr{B}\}$ and all the $\{\mathscr{B}_\gamma\}$ are simple on U, respectively $U \times V$. Then*

$$\textstyle\sum_\gamma \boldsymbol{i}[(A \times V) \cap B, \mathscr{B}_\gamma; U \times V] = [B : B_1]\, \boldsymbol{i}(A \cap B_1, \mathscr{B}; U).$$

Proof. As to the dimensions, all the symbols are defined. Furthermore, we note that the projections on U of the maximal connected bunches of $(A \times V) \cap B$ are either entirely contained in $\{\mathscr{B}\}$ or do not have any point in common with $\{\mathscr{B}\}$.

We proceed by induction on the maximum of the excess of $\mathscr{B}$ and the excess of the $\mathscr{B}_\gamma$. If this is zero, then the theorem is true ([VI], Chap. VII, Th. 8).

Let k be an algebraically closed field of definition for U, V, A and B. Let $\alpha = [X, Y, K, Q'; A, U, k]$ be a system having the properties mentioned in Prop. 1, $Y(Q') = A + \sum_\lambda \eta_\lambda A_\lambda$; let $\mathscr{D}_{\lambda i}$ be those maximal connected bunches of $A_\lambda \cap B_1$ which are in $\{\mathscr{B}\}$. We have by Prop. **1iib.**, $\mathscr{D}_{\lambda i} \prec \mathscr{B}$. For Q generic on X over K, we have that $Y(Q) = A^*$, with $A^* \cdot B_1 = \sum_i R_i$, is $K(Q)$-prime rational. Let $\sum_i R'_i$ be a specialization of $\sum_i R_i$ over the specialization $Q \rightarrow Q'$, with reference to K; let σ be the number of points of $\sum_i R'_i$ which are in $\{\mathscr{B}\}$. Then we have by the definition of the $\boldsymbol{i}$-symbol.

$$(1) \qquad \boldsymbol{i}(A \cap B, \mathscr{B}; U) = \sigma - \textstyle\sum_\lambda \eta_\lambda \sum_i \boldsymbol{i}(A_\lambda \cap B_1, \mathscr{D}_{\lambda i}; U).$$

Next, consider the variety X and the subvariety $Y \times V$ of $X \times U \times V$. We will show that they have, with respect to the variety B, the variety $U \times V$ and every one of the bunches $\mathscr{B}_\gamma$, the properties mentioned in Th. 3. Write $Z = Y \times V$ and let again Q be generic on X over K. Then $Z(Q) = Y(Q) \times V$ by [VI], Chap. VI, Th. 7. $Z(Q)$ is of the required dimension $n + m - b$. Since $Y(Q) \cdot B_1 = \sum_i R_i$, with (by Prop. **1i.**) R_i generic on B_1 over K, it follows (since $[B : B_1] \neq 0$) that $[Y(Q) \times V] \cap B$

consists of generic points on B. Hence we can write $Z(Q)\cdot B=\sum_i\sum_j T_{ij}$, $j=1,\cdots,[B:B_1]$, $\mathrm{pr}_U T_{ij}=R_i$. Again by [VI], Chap. VI, Th. 7, we have $Z(Q')=Y(Q')\times V=A\times V+\sum_\lambda \eta_\lambda(A_\lambda\times V)$. Let $\mathcal{D}_{\lambda ih}$ be those maximal connected bunches of $(A_\lambda\times V)\cap B$ which project into $\{\mathcal{D}_{\lambda i}\}$ (as point sets); then (in view of the fact that $\mathcal{D}_{\lambda i}\prec\mathcal{B}$ and by applying Prop. **1iib.** to the projection on U of every component of the bunches $\mathcal{B}_\gamma$) it follows that there is to every $\mathcal{D}_{\lambda ih}$ a certain $\mathcal{B}_\gamma$ such that $\mathcal{D}_{\lambda ih}\prec\mathcal{B}_\gamma$. Moreover, the bunches $\mathcal{D}_{\lambda ih}$ contain all the components of $(A_\lambda\times V)\cap B$ which have points in common with the $\{\mathcal{B}_\gamma\}$ for some γ since the $\mathcal{D}_{\lambda i}$ contain all the components of $A_\lambda\cap B_1$ which have points in common with $\{\mathcal{B}\}$.

Let $\sum_{i,j}T'_{ij}$ be a specialization of $\sum_{i,j}T_{ij}$ over the specialization $(Q,\sum_i R_i)\to(Q',\sum_i R'_i)$ with reference to K. Then we have $\mathrm{pr}_U T'_{ij}=R'_i$; hence $T'_{ij}\in\{\mathcal{B}_\gamma\}$ for some γ if and only if $R'_i\in\{\mathcal{B}\}$. Therefore, the number of points of $\sum_{i,j}T'_{ij}$ which are in $\{\mathcal{B}_\gamma\}$ for some γ is equal to $[B:B_1]\sigma$. An application of Th. 3 to the subvariety B of $U\times V$, to every one of the bunches $\mathcal{B}_\gamma$, to the varieties X and $Y\times V$ on $X\times U\times V$ and to the specialization $(Q,\sum_{i,j}T_{ij})\to(Q',\sum_{i,j}T'_{ij})$ over K gives

$$(2)\qquad \sigma[B:B_1]=\textstyle\sum_\gamma \boldsymbol{i}[(A\times V)\cap B,\mathcal{B}_\gamma;U\times V]\\ +\textstyle\sum_\lambda\eta_\lambda\sum_{i,h}\boldsymbol{i}[(A_\lambda\times V)\cap B,\mathcal{D}_{\lambda ih};U\times V].$$

Since, as we have seen above, $\mathcal{D}_{\lambda i}\prec\mathcal{B}$ and every $\mathcal{D}_{\lambda ih}\prec\mathcal{B}_\gamma$ for some γ, we can apply, by our induction hypothesis, the theorem to B, to $A_\lambda\times V$, and to the bunches $\mathcal{D}_{\lambda i}$ and $\mathcal{D}_{\lambda ih}$. Hence

$$(3)\qquad [B:B_1]\boldsymbol{i}(A_\lambda\cap B_1,\mathcal{D}_{\lambda i};U)=\textstyle\sum_h\boldsymbol{i}[(A_\lambda\times V)\cap B,\mathcal{D}_{\lambda ih};U\times V]$$

Summation over all λ, i and substitution into (2) gives

$$[B:B_1]\cdot[\sigma-\textstyle\sum_\lambda\eta_\lambda\sum_i\boldsymbol{i}(A_\lambda\cap B_1,\mathcal{D}_{\lambda i};V)]=\sum_\gamma\boldsymbol{i}[(A\times V)\cap B,\mathcal{B}_\gamma;U\times V].$$

From this, one obtains, by using (1), the required formula.

THEOREM 5 (Associativity formula). *Let A^a, B^b and C^c be subvarieties of a projective variety V^n $(a+b+c=2n)$; let $\mathcal{G}$ be a maximal connected bunch of $A\cap B\cap C$ such that every point of $\{\mathcal{G}\}$ is simple on V. Suppose that all the components D_σ of $A\cap B$ which have points in common with $\{\mathcal{G}\}$ are proper and, similarly, let all the components E_τ of $B\cap C$ which have points in common with $\{\mathcal{G}\}$ be proper. Let $\mathcal{D}_{\sigma j}$, respectively $\mathcal{E}_{\tau j}$, be those maximal connected bunches of $D_\sigma\cap C$, respectively $A\cap E_\tau$, which have points in common with $\{\mathcal{G}\}$. Then*

$$\textstyle\sum_\sigma\boldsymbol{i}(A\cdot B,D_\sigma;V)\sum_j\boldsymbol{i}(D_\sigma\cap C,\mathcal{D}_{\sigma j};V)\\ =\textstyle\sum_\tau\boldsymbol{i}(B\cdot C,E_\tau;V)\sum_j\boldsymbol{i}(A\cap E_\tau,\mathcal{E}_{\tau j};V).$$

Proof. First of all we observe that the maximal connected bunches of $D_\sigma \cap C$ and $A \cap E_\tau$ are either entirely inside or entirely outside $\{\mathscr{G}\}$. We proceed by induction on the excess of $\mathscr{G}$ (i.e., the maximum of the integers dim. G for all components G of $\mathscr{G}$). If the excess $\mathscr{G} = 0$ then the theorem is a special case of [VI], Chap. VI, Th. 5.

Let k be a field of definition for A, B, C, and V. Let

$$\alpha = [U, W, K_1, P'; A, V, k] \text{ and } \gamma = [X, Y, K_2, Q'; C, V, k]$$

be systems having the properties mentioned in Proposition 1; moreover, we assume that K_1 and K_2 are free with respect to each other over k. Let K be the algebraic closure of the compositum of K_1 and K_2.

We have, by assumption,

$$W(P') = A + \sum_{\lambda=1} \eta_\lambda A_\lambda \text{ and } Y(Q') = C + \sum_{\mu=1} \pi_\mu C_\mu;$$

for convenience of notation, we will write $W(P') = \sum_\lambda \eta_\lambda A_\lambda$, where it is understood (during the proof of this theorem) that without further references, the summation starts with $\lambda = 0$, where $\eta_0 = 1$ and $A_0 = A$. Similarly, we write $Y(Q') = \sum_\mu \pi_\mu C_\mu$ with $\pi_0 = 1$ and $C_0 = C$. Let $D_{\lambda\sigma}$ and $E_{\mu\tau}$ be those components of $A_\lambda \cap B$, respectively $B \cap C_\mu$, which have points in common with $\{\mathscr{G}\}$; again we denote D_σ by $D_{0\sigma}$ and E_τ by $E_{0\tau}$. Since D_σ and E_τ are proper components of $A \cap B$, respectively $B \cap C$, it follows by the properties of the systems α and γ (see Prop. 1**ii.**) that all $D_{\lambda\sigma}$ and $E_{\mu\tau}$ are proper components of intersection of $A_\lambda \cap B$, respectively $B \cap C_\mu$ on V. Furthermore, it follows also by the properties of the systems α and γ that (see Prop. 1**ii.**) the maximal connected bunches of $A_\lambda \cap B \cap C$, of $A \cap B \cap C_\mu$ and of the $A_\lambda \cap B \cap C_\mu$ are either strictly contained in $\{\mathscr{G}\}$, or do not have any point in common with $\{\mathscr{G}\}$. Let $\mathscr{D}_{\lambda\sigma\mu j}$, respectively $\mathscr{E}_{\mu\tau\lambda j}$, be those maximal connected bunches of $D_{\lambda\sigma} \cap C_\mu$, respectively $A_\lambda \cap E_{\mu\tau}$, which have points in common with $\{\mathscr{G}\}$. (Similarly to the above, we choose notations such that $\mathscr{D}_{0\sigma 0 j} = \mathscr{D}_{\sigma j}$ and $\mathscr{E}_{0\tau 0 j} = \mathscr{E}_{\tau j}$.)

Let P and Q be independent generic points on U and X over K. Write $W(P) = A^*$ and $Y(Q) = C^*$; by assumption on the systems α and γ (and since K_1 and K_2 are free with respect to each other over k), we have that $A^* \cdot B \cdot C^* = \sum_i S_i$ is a $K(P, Q)$-rational cycle. Let H be the locus of (P, Q, S_i) over K; $H \subset U \times X \times V$. Since $S_i \in A^* \cdot B \cdot C^*$ it follows from the fact that $A^* \to \sum_\lambda \eta_\lambda A_\lambda$ and $C^* \to \sum_\mu \pi_\mu C_\mu$ over the specialization $(P, Q) \to (P', Q')$ with reference to K, by [III], page 53g, that the maximal connected bunches of $H\{P', Q'\}$ are contained in the maximal connected bunches of $A_\lambda \cap B \cap C_\mu$ ($\lambda = 0$ and $\mu = 0$ included). By our observations, it follows that those bunches are either entirely inside or entirely outside $\{\mathfrak{G}\}$. Apply [II], Th. 3 to the variety H on $U \times X \times V$, to the simple point (P', Q') on $U \times X$ and to those maximal connected bunches of $H\{P', Q'\}$ which are in $\{\mathfrak{G}\}$; it then follows that the number of points of every specialized cycle of $\sum_i S_i$, over the specialization $(P, Q) \rightarrow (P', Q')$ with reference to K, which are in $\{\mathfrak{G}\}$ is always the same. Consider the specialization $(P, Q, \sum_i S_i) \rightarrow (P, Q', \cdot\cdot\cdot) \rightarrow (P', Q', \sum_i S'_i)$ over K; let n' be the number of points of $\sum_i S'_i$ which are in $\{\mathfrak{G}\}$. Let n'' be the corresponding number for the cycle $\sum_i S''_i$, where $(P, Q, \sum_i S') \rightarrow (P', Q, \cdot\cdot\cdot) \rightarrow (P', Q', \sum_i S''_i)$ over K. As we have seen,

$$n' = n'' \tag{1}$$

Next we note that all the $A^* \cdot E_{\mu\tau}$ are defined, as follows from the assumption on the system α and from the fact that K_2 (over which the $E_{\mu\tau}$ are defined) and K_1 are free with respect to each other over k. (Furthermore, we keep in mind that the components of the $B \cap C_\mu$, except the $E_{\mu\tau}$, are entirely outside $\{\mathfrak{G}\}$.) Apply Th. 3 to every variety $E_{\mu\tau}$, to U and W on $U \times V$ and to those maximal connected bunches of $A_\lambda \cap E_{\mu\tau}$ which are in $\{\mathfrak{G}\}$. We obtain after a summation

$$n' = \textstyle\sum_{\mu,\tau} \pi_\mu \boldsymbol{i}(C_\mu \cdot B, E_{\mu\tau}; V) \cdot \sum_{\lambda,h} \eta_\lambda \boldsymbol{i}(A_\lambda \cap E_{\mu\tau}, \mathcal{E}_{\mu\tau\lambda h}; V). \tag{2}$$

Similarly, one has

$$n'' = \textstyle\sum_{\lambda,\sigma} \eta_\lambda \boldsymbol{i}(A_\lambda \cdot B, D_{\lambda\sigma}; V) \cdot \sum_{\mu,j} \pi_\mu \boldsymbol{i}(D_{\lambda\sigma} \cap C_\mu, \mathcal{D}_{\lambda\sigma\mu j}; \mathrm{V}) \tag{3}$$

Suppose we take a pair λ, μ but not the pair $\lambda = 0$ and $\mu = 0$ (at the same time). As we have already observed above, those maximal connected bunches of $A_\lambda \cap B \cap C_\mu$ which have points in common with $\{\mathfrak{G}\}$ are strictly contained componentwise in $\{\mathfrak{G}\}$. Therefore, by our induction hypothesis, we can apply the theorem to every such bunch. After a summation (over all the maximal connected bunches of $A_\lambda \cap B \cap C_\mu$ which are in $\{\mathfrak{G}\}$, λ and μ fixed), we obtain

$$\begin{aligned} \textstyle\sum_\sigma \boldsymbol{i}(A_\lambda \cdot B, D_{\lambda\sigma}; V) \cdot \sum_j \boldsymbol{i}(D_{\lambda\sigma} \cap C_\mu, \mathcal{D}_{\lambda\sigma\mu j}; V) \\ = \textstyle\sum_\tau \boldsymbol{i}(B \cdot C_\mu, E_{\mu\tau}; V) \cdot \sum_h \boldsymbol{i}(A_\lambda \cap E_{\mu\tau}, \mathcal{E}_{\mu\tau\lambda h}; V). \end{aligned} \tag{4}$$

(4) holds for all pairs (λ, μ), except for the pair $(0, 0)$. However then, from (1), (2), (3) and (4), and since $\eta_0 = 1$ and $\pi_0 = 1$, it follows that (4) is also true for $\lambda = 0$ and $\mu = 0$. Since $A_0 = A$, $C_0 = C$, $D_{0\sigma} = D_\sigma$, $E_{0\tau} = E_\tau$, $\mathcal{D}_{0\sigma 0 j} = \mathcal{D}_{\sigma j}$ and $\mathcal{E}_{0\tau 0 h} = \mathcal{E}_{\tau h}$, this is the required result.

From the above theorems, and from the theorem corresponding to [VI], Chap. VI, Th. 7 which can be proved by the above developed methods, many of the usual properties of the i-symbol can be derived, for instance, the analogous result to [VI], Chap. VI, Th. 9 (see the proof of that theorem in [VI]).

UNIVERSITY OF LEYDEN, THE NETHERLANDS.

REFERENCES.

[I] W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, vol. II, Cambridge, 1952.

[II] J. P. Murre, "On a connectedness theorem for birational transformations at a simple point," *American Journal of Mathematics*, vol. 80 (1958), pp. 3-15.

[III] P. Samuel, "Méthodes d'Algèbre Abstraite en géométrie Algébrique," *Ergebnisse der Mathematik*, Neue Folge, Heft 4 (1955), Berlin.

[IV] F. Severi, "Ueber die Grundlagen der algebraischen Geometrie," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 9 (1933), pp. 335-364.

[V] B. L. van der Waerden, "Zur algebraischen Geometrie, XIV," *Mathematische Annalen*, vol. 115 (1938), pp. 619-642.

[VI] A. Weil, *Foundations of Algebraic Geometry*, New York, 1946.

[VII] ———, "Sur les critères d'équivalence en géométrie algébrique," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[VIII] O. Zariski, "Theory and applications of holomorphic functions on algebraic varieties over arbitrary groundfields," *Mèmoirs of the American Mathematical Society*, No. 5 (1951).

[IX] ———, "The connectedness theorem for birational transformations," *Princeton Series No. 12* (1957), pp. 182-188.

EXTENSION OF REPRESENTATIONS OF LIE GROUPS, II.*

By G. D. Mostow.[1]

1. **Introduction.** This paper is a sequel to "Extension of Representations of Lie Groups and Lie Algebras, I" by G. Hochschild and G. D. Mostow (hereafter referred to as ERI). In ERI, some simple but basic constructions of representation spaces are introduced, and thereby one can analyze almost completely the problem of extending a (finite dimensional) representation of a normal analytic subgroup G of an anaytic group L to a representations of L in the case that there is an analytic subgroup Q with $L = QG$ and $Q \cap G$ compact. Indeed, from the extension theorem in this special situation, one deduces quickly all the standard results on faithful representations of Lie groups (see ERI).

This paper is devoted to the more general extension problem of extending a representation from a normal closed connected subgroup G to an analytic group L with $L \supset G$. The analogue of this problem for Lie algebras presents no difficulties at all, once one has resolved the special case of extending from an ideal G to a semi-direct sum $Q + G$, because one can reconstruct a Lie algebra L from an ideal G by successive formation of semi-direct sums. By contrast, the extension methods of ERI do not suffice to settle the more general extension problem—essentially for topological reasons. (See Sec. 2, Remark 2.8). In addition to the methods of ERI, we require one additional extension method in order to be able to overcome the topological complications that arise. The method presented here relies heavily on the theory of algebraic groups and, in particular, on the author's previous results on fully reducible subgroups of algebraic groups. The main theorem of this paper (see Sec. 3) provides a complete solution to the extension problem for closed normal connected subgroups of analytic groups.

It is a pleasure to acknowledge my debt to Dr. Gerhard Hochschild with whom I have had many stimulating conversations on topics treated here.

2. **Preliminaries.** Let G be a Lie group. We denote by G_1 the connected component of the identity element. We denote by $G^{\cdot}$ the Lie algebra

---

* Received June 17, 1957.

[1] Performed under Contract AF18(600)1474 with the Office of Scientific Research and Development of the U. S. Air Force.

of G and identitfy $G^{\cdot}$ with the tangent space to G at the identity element. If ρ is a homomorphism of G, we denote by $\rho^{\cdot}$ the differential of ρ at the identity element so that $\rho^{\cdot}$ is the induced homomorphism of $G^{\cdot}$. We denote by Aut G and Aut $G^{\cdot}$ the group of automorphisms of G and $G^{\cdot}$ respectively. The map $x \rightarrow x^{\cdot}$ of Aut G into Aut $G^{\cdot}$ is one-to-one, and it is a homeomorphism when Aut G is given the compact open topology and Aut $G^{\cdot}$ is given its topology relative to the full linear group or, equivalently, its Lie group topology [4]. If G is an analytic *real linear* group, that is, an analytic subgroup of the full linear group $GL(V)$ of some real linear space V, then we shall have to distinguish between its analytic group topology and its topology relative to the full linear group $GL(V)$. Accordingly, if $F \subset G$, we denote by F^G the topological closure of F in the analytic group topology of G and by $\bar{F}$ the closure in the full linear group. It is known that $F^G \subset \bar{F}$ if $F \subset G$, so that $(\bar{C} \cap G)^G = \bar{C} \cap G$ for any subset C of the full linear group. If G is a Lie subgroup of the full linear group $GL(V)$, we can indentify the Lie algebra $G^{\cdot}$ with a subset of the linear space $E(V)$ of all endomorphisms on V, by the usual rule for identifying the tangent space to a submanifold of a linear space E with a subspace of E. When $G^{\cdot}$ is thus identified with a subspace of $E(V)$, the adjoint operation Ad x, for $x \in G$, coincides with the restriction of the conjugation $C(x): y \rightarrow xyx^{-1}$ $(y \in E(V))$ to $G^{\cdot}$, because $(C(x))^{\cdot} = C(x)$.

We use the term "representation" to mean "finite dimensional representation." By an *algebraic group* we mean here a group G of invertible endomorphisms of a finite dimensional real or complex linear space V, such that G is the intersection of the full linear group with an algebraic manifold in the linear space $E(V)$ of all endomorphisms of V. An *algebraic Lie algebra* is the Lie algebra of an algebraic group. By a *rational representation* of a subgroup $G \subset GL(V)$ we mean a (finite dimensional) representation of G which is the restriction to G of a representation ρ of an algebraic group L such that $L \supset G$ and ρ is a rational map. If $G \subset GL(V)$, we denote by G^* the topologically connected component of the identity of the smallest algebraic group containing G. In general, G^* is not an algebraic group. If ρ is a rational representation of an algebraic group L, then $\rho(L)$ need not be algebraic. However $\rho^{\cdot}(L^{\cdot})$ is an algebraic Lie algebra ([2], p. 140). It follows immediately that $\rho(G^*) = \rho(G)^*$ for any rational representation of G.

If t is an endomorphism of any finite dimensional linear space V over a perfect field, there is a unique semi-simple (i. e. fully reducible) element s and a unique nilpotent element n such that $t = s + n$ and $sn = ns$. If t is invertible, then s is also invertible and $t = su$ where u is the *unipotent* (i.e., $u - 1$ is nilpotent) element $1 + s^{-1}n$. The representation $t = su$ with s semi-simple, u unipotent, and $su = us$ is unique; it is called the *Jordan product decomposition* (see [2], p. 71, Th. 7). The endomorphism s is called *the semi-simple part of* t and is denoted by t'. An algebraic group which contains t contains t' also ([2], p. 184). A rational representation sends semi-simple endomorphisms into semi-simple endomorphisms, unipotent endomorphisms into unipotent endomorphisms ([8]), and therefore $\rho(t') = \rho(t)'$.

A set U of endomorphisms of a linear space V is called a *unipotent family* if there is a series of subspaces $V_0 = V_1 \subset \cdots \subset V_n = V$, each invariant under U, such that the V_i/V_{i-1} part of U consists of the identity element, $i = 1, \cdots, n$. A representation ρ of a group G is called *unipotent* if $\rho(G)$ is a unipotent family. A group of unipotent endomorphisms of a linear space is a unipotent family ([5], Sec. 2).

Remark 2.1. If M and N are algebraic Lie algebras with $[M, N] \subset N$, then $M + N$ is algebraic ([8], Sec. 4.4, p. 209). From this it follows that if M and N are analytic linear groups with N invariant under conjugations from M and $N = N^*$, then $(MN)^* = M^*N$.

Remark 2.2. A Lie algebra of nilpotent endomorphisms is algebraic ([2], pp. 181-183). An algebraic group of unipotent elements is algebraically-connected (or "algebraically-irreducible"; i.e., the associated ideal is prime) ([2], p. 183) and is, in fact, topologically connected since each element in it is the exponential of an element from the Lie algebra. In particular, an analytic group of unipotent elements is algebraic and a fortiori closed.

Remark 2.3. Let G be an algebraic Lie group, let M be any maximal fully reducible subgroup of G and let U be the maximum normal algebraically-connected subgroup of unipotent elements in G. Then $G = M \cdot U$ (semi-direct) ([8], Th. 7.1). If G is algebraically-connected, then any fully reducible subgroup of G is conjugate to a subgroup of M by an inner automorphism from $(U \cap G')_1$ ([8], Th. 7.1, Th. 4.1), where G' denotes the commutator subgroup of G. By Remark 2.2, $U^* = U_1 = U$ and therefore $G_1 = M_1 \cdot U$ (semi-direct). It follows from the foregoing that any fully reducible subgroup of G_1 is conjugate to a subgroup of M_1 by an inner automorphism from $(U \cap G')_1$.

If P is a fully reducible subgroup of G_1 and U is a normal analytic group of unipotent elements with $G_1 = PU$, then P is maximal fully reducible in G_1. For let Q be a fully reducible subgroup of G containing P. Then

$Q = P(Q \cap U)$. But $Q \cap U$ is normal in Q and therefore fully reducible. Simultaneously, it is a unipotent family. Hence it consists of the identity alone and $P = Q$. A similar argument shows that U is the maximum analytic normal subgroup of unipotent elements.

A rational representation carries fully reducible groups into fully reducible groups ([8]).

Remark 2.4. If S is an analytic semi-simple linear group, then $S^* = S$. For let $S^\cdot$ denote the Lie algebra of S. The commutator subalgebra $[S^\cdot, S^\cdot]$ is an algebraic Lie algebra ([2], p. 177). Hence $S^\cdot = [S^\cdot, S^\cdot]$ is algebraic and therefore S is the connected component of the identity of the algebraic group hull of S. Consequently $S^* = S$. In particular, S is closed in the full linear group. The center of S is finite, as can be seen in a variety of ways.

Remark 2.5. Let L be an analytic group and let P denote the intersection of the kernels of all finite dimensional representations of L. Then L/P has faithful representation, by a result of Goto (see [3] or [5]).

Remark 2.6. Let L be an analytic group. As is well-known, L is topologically the direct product of a maximal compact subgroup and a euclidean space; moreover, any compact subgroup is conjugate to a subgroup of any maximal one. If G is a closed normal analytic subgroup, and L/G is compact, then $L = QG$ for any maximal compact subgroup Q. This is a result of Malcev ([7], Th. 10, p. 180), but since we require it only in the special case that L/G is solvable, we present the following brief proof for the reader's convenience. The group L/G, being a compact solvable analytic group, is abelian, as is seen from considering its adjoint representation. Therefore QG is normal, and $L/QG = (L/G)/(QG/G)$ is again a toroid. But $L/QG = (L/Q)(QG/Q)$ is the image of the euclidean spaceL/Q by a continuous and open mapping with the inverse image of each point homeomorphic to the connected set QG/Q. Therefore L/QG is a *simply connected* toroid. Hence it is a point and $L = QG$. A part of our argument establishes that L/F is simply connected if F is a closed analytic subgroup containing a maximal compact subgroup of L.

Remark 2.7. Let ρ be a representation of an analytic group G on a real or complex linear space V. Let $V_0 \subset V_1 \subset \cdots \subset V_n = V$ be a sequence of linear subspaces of V invariant under $\rho(G)$ such that the V_i/V_{i-1} part of ρ is irreducible, $i = 1, \cdots, n$. Let ρ' denote the representation induced by ρ on the direct sum $V_1/V_0 + \cdots + V_n/V_{n-1}$. Then ρ' is semi-simple (i.e. fully reducible) and it is independent of the original choice of the subspaces $\{V_i\}$ up to an isomorphism ([5] or [6]); ρ' is called the *associated semi-simple representation of* ρ. We consistently denote the commutator subgroup of L by L' or by $[L, L]$. By the *radical* of an *analytic group* L, we consistently mean the analytic subgroup T whose Lie algebra $T^{\cdot}$ is the radical of the Lie algebra $G^{\cdot}$.

Let ρ be a representation of an analytic group G on a real or complex linear space V, and let G be a subgroup of an analytic group L. Let σ be a representation of L on a real or complex linear space W. σ is called an *extension* of ρ if there is a monomorphism θ of V into W such that $\theta \cdot \rho(g) = \sigma(g) \cdot \theta$ for all $g \in G$.

The main extension results in ERI can be stated as follows: *Let G be a closed normal analytic subgroup of an analytic group L. Let Q be an analytic subgroup of L such that $Q \cap G$ is compact. Assume that there is a representation of Q which is faithful on $Q \cap G$. Let ρ be a representation of G. A necessary and sufficient condition that ρ can be extended to a representation of the analytic group QG is the following Condition* a),

Condition a). $\rho'(yxy^{-1}x^{-1}) = 1$ for all y in QG and x in the radical of G.

Moreover, the extended representation σ can be chosen in such a way that the kernel of σ' contains the kernel of ρ' (ERI Theorem 3.2). *If Q satisfies the additional Condition* b),

Condition b). (i) $\rho'(qgq^{-1}g^{-1}) = 1$ for all $q \in Q$ and $g \in G$; and (ii) the $G^{\cdot}$-part of $\operatorname{Ad} q$ is unipotent for all $q \in Q$,

then σ can be so chosen that the kernel of σ' contains Q as well as the kernel of ρ'. (ERI, Section 6)

Condition a) is clearly implied by

Condition a'). *ρ' is trivial on $N \cap G$, where N is the radical of the commutator subgroup of L.* Conversely, if ρ can be extended to a representation σ of L, then ρ' is trivial on $N \cap G$. For σ is unipotent on N, as is well known, so that σ' is trivial on the normal subgroup N (ERI, Sec. 2), and consequently ρ' is trivial on $N \cap G$.

If $Q \subset N$, and ρ satisfies Condition a'), then Q satisfies Condition b). We can now assert the following remark.

Remark 2.8. *Let L, G, N, Q, be as in Remark* 2.7. *Assume that ρ' is trivial on $N \cap G$. Then ρ can be extended to a representation σ of QG*

such that the kernel of σ' *contains the kernel of* ρ' *and also the subgroup* Q *if* $Q \subset N$.

We note that if $Q \subset N$, then σ' is trivial on $Q(N \cap G) = N \cap QG$. This raises the possibility of extending ρ from G to L in *two stages*: from G to NG, by recursively selecting $Q \subset N$; and then from NG to L. The obstruction to this procedure occurs in two places. In the first place NG need not be closed; the passage from NG to L suggests that an additional condition must be imposed on ρ. In the second place, even assuming that NG is closed, it may be possible to select a non trivial $Q \subset N$ so that $Q \cap G$ is compact. The essential contribution of this paper is to show how to extend ρ from G to $\overline{GN}$.

3. A determination of ρ'.

LEMMA 3.1. *Let* G *be an analytic group. For* $x \in G$, *let* $\mathrm{Ad}\, x$ *denote the differential at the identity element of the inner automorphism* $g \rightarrow xgx^{-1}$. *Then every element in* $(\mathrm{Ad}\, G)^*$ *is the differential at the identity of an automorphism of* G *which keeps fixed each central element of* G.

Proof. Clearly, no generality is lost in assuming G to be simply connected. By Ado's theorem, there exists a faithful representation of the Lie algebra of G. Let ρ denote the corresponding representation of G and let K denote its kernel.

Let F denote the tangent space to $\rho(G)$ at the identity element. We identify it (see Sec. 2) with a Lie subalgebra of the Lie algebra E of all endomorphisms of the underlying linear space V. The conjugations $C(x)$, $y \rightarrow xyx^{-1}$, of E clearly keep $F^{\cdot}$ invariant when $x \in \rho(G)$, and consequently $F^{\cdot}$ is invariant under the conjugations from the algebraic group hull of $\rho(G)$. Define $\beta(x)$ as the restriction of $C(x)$ to $F^{\cdot}$ on the group A of all automorphisms of V with $C(x)F^{\cdot} = F^{\cdot}$. Clearly, A is an algebraic group, β is a rational representation and $\rho(G) \subset A$. Therefore $\rho(G)^* \subset A$ and $\beta(\rho(G)^*) = (\beta(\rho(G)))^*$. It is easily verified that $\beta(x)$ coincides with the differential at the identity element of the restriction of $C(x)$ to $\rho(G)$ and that $C(x)\rho(G) = \rho(G)$ whenever $C(x)F^{\cdot} = F^{\cdot}$. Thus $\beta(\rho(G)) = \mathrm{Ad}\,\rho(G)$ and $\beta(\rho(G)^*) = (\mathrm{Ad}\,\rho(G))^*$. But $\rho(G)^*$ is contained in the centralizer of the center of $\rho(G)$. Thus each automorphism in $(\mathrm{Ad}\,\rho(G))^*$ is induced by an automorphism of $\rho(G)$ keeping fixed each central element. Lifting these automorphisms of $\rho(G)$ to a set of automorphisms, A, of the simply connected group G, we find that each element of $(\mathrm{Ad}\, G)^*$ is the differential at the identity element of an automorphism keeping invariant the discrete set zK for each z in the center of G. Since the set A is a connected family of transformations of G and contains the identity, it leaves each element of zK fixed. Proof of Lemma 3.1 is now complete.

LEMMA 3.2. *Let G be an analytic linear group and N a normal subgroup closed in the analytic group topology of G. Then N is normal in G^*.*

Proof. The group N_1 is connected and closed in G and is therefore analytic. Let $G^{\cdot}$ and $N^{\cdot}$ denote the Lie algebras of G and N respectively; we identify their elements with endomorphisms of the underlying linear space V in the usual way. For any automorphism x of V, let $C(x)$ denote conjugation by x, and let A be the set of all automorphisms x of V such that $C(x)N^{\cdot}=N^{\cdot}$. Clearly A is an algebraic group. It is also clear that $xN_1x^{-1}=N_1$ if and only if $C(x)N^{\cdot}=N^{\cdot}$. Accordingly, $G\subset A$. From this, $G^*\subset A$. Hence N_1 is normal in G^*. By the same reasoning, G is normal in G^*. Let $\beta(x)$ denote the $G^{\cdot}/N^{\cdot}$ part of $C(x)$ for $x\in G^*$. Then β is a rational representation of G^* and thus $\beta(G^*)=\beta(G)^*=(\operatorname{Ad} G/N_1)^*$. Let $\alpha(x)$ denote the automorphism of G/N_1 that is induced by $C(x)$ for $x\in G^*$. Then $\alpha(G^*)^{\cdot}=\beta(G^*)=(\operatorname{Ad} G/N_1)^*$. Applying Lemma 3.1, each element in $\alpha(G)^{\cdot}$ is the differential of an automorphism of G/N_1 keeping each central element fixed. Since $x\rightarrow x^{\cdot}$ is a monomorphism of $\operatorname{Aut} G/N_1$ into $\operatorname{Aut}(G/N_1)^{\cdot}$, each automorphism in $\alpha(G^*)$ keeps each central element of G/N_1 fixed. Since N/N_1 is a discrete normal subgroup in G/N_1, it is central. Hence $\alpha(G^*)(N/N_1)=N/N_1$ and $C(G^*)\cdot N=N$. That is, N is normal in G^*.

Note. It is curious that Lemma 3.2 can be proved trivially when N is is connected and requires so complicated a proof for N not connected.

LEMMA 3.3. *Let L be an analytic linear group, let G be a normal analytic subgroup closed in L, let T be the radical of G, let H be an analytic subgroup whose Lie algebra is a Cartan subalgebra of the Lie algebra of T, let N be the radical of the commutator subgroup L', and let D be a maximal compact subgroup of $(H^*\cap(TN)^L)_1$. Then*

1. *D is a maximal compact subgroup in DTN.*

2. *$(TN)^L=DTN$.*

3. *$(GN)^L=DGN$.*

4. *$HN\cap D$ is dense in D.*

5. *DG contains a maximal compact subgroup of $(GN)^L$, and $N\cap DG$ is connected.*

Proof. It is known (see [9] Lemma 2, p. 7) that $T=HT'$ and, by definition, $T'\subset N$. Hence $TN=HN$ and $(TN)^L\subset(TN)^*=(HN)^*$. Now the Lie algebra of N consists of nilpotent endomorphisms, as is well known. Hence $N^*=N$ by Remark 2.2 and $(HN)^*=H^*N$ by Remark 2.1. Now $H^*=M\cdot U$ where M is a maximal fully reducible subgroup of H^* containing D and U is the maximum analytic normal subgroup of unipotent elements. Hence $(TN)^L\subset(M\cdot U)N=M(UN)$, where the elements of UN are unipotent by Lie's theorem on simultaneous triangularizing. Therefore M is a maximal fully reducible subgroup in $(TN)^L$, by Remark 2.3. Let C be a connected compact subgroup of $(TN)^L$ with $C\supset D$. By Remark 2.3, there is an element $x\in((TN)^{*\prime}\cap N)_1=((TN)'\cap N)_1$ such that $xCx^{-1}\subset M$. Then, for every $d\in D$, $xdx^{-1}=m(d)\in M$ implies $dx^{-1}=x^{-1}m$ $=m(m^{-1}x^{-1}m)$. Hence $d=m(d)=xdx^{-1}$ and $xDx^{-1}=D$. Therefore $D\subset xCx^{-1}\subset(M\cap(TN)^L)_1\subset(H^*\cap(TN)^L)_1$, and, by its maximality, $D=xCx^{-1}$. Hence $D=C$, and D is a maximal compact subgroup in $(TN)^L$, because a maximal compact subgroup of $(TN)^L$ is connected.

Proof of 2. Let J denote the simply connected covering group of $(TN)^L$, let π denote the covering homomorphism, and let $K=\pi^{-1}(D)$. Then J/K $=(TN)^L/D$, and the latter is simply connected since an analytic group is topologically the direct product of any maximal compact group and a euclidean space. Consequently, K is connected. Hence $\pi^{-1}(DTN)$, being a connected normal analytic subgroup of a simply connected Lie group, is closed. It follows immediately that DTN is closed in L and equals $(TN)^L$.

Proof of 3. Let SR be a Levi decomposition for $(GN)^L$, S being semi-simple and R the radical. $S\cap R$ is a discrete normal subgroup of the analytic group S and is therefore central in S. Inasmuch as the center of a semi-simple analytic linear group is finite, $S\cap R$ is finite. Let λ denote the epimorphism $s\cdot r\rightarrow sr$ of the semi-direct product $S\cdot R$ onto SR. The kernel of λ consists of all elements $x\cdot x^{-1}$ with $x\in S\cap R$ and is thus finite. Consequently, an analytic subgroup A which contains S is closed in SR if and only if the connected component $(A\cap R)_1$ is closed in R.

The semi-simple analytic group S is contained in DGN since

$$S=[S,S]\subset[(GN)^L,(GN)^L]\subset[(GN)^*,(GN)^*]\subset[GN,GN]\subset GN.$$

Moreover, $(DGN\cap R)_1=DTN$ and is closed in L by part 2 above. Hence $(DTN)^R=DTN$, and $(DGN)^L=DGN$.

Proof of 4. Recall that N is the radical of the commutator group L' and therefore DHN/N is an abelian analytic group. Therefore it is a direct product $C\cdot W$, where C is its maximum compact subgroup and W is a vector group which clearly can be taken to be a subgroup of HN/N. It is known (Remark 2.6) that the preimage of C contains a compact subgroup mapping onto C. Since D is a maximal compact subgroup of DHN, we deduce that D projects onto C. Let V denote the preimage of W. Then $DHN = DV$ with V closed and simply conencted, and $D \cap V \subset N$. Since $D \cap V$ is a compact group of unipotent elements, it contains the identity alone. Hence the epimorphism of the semi-direct product $D\cdot V$ onto DV is a monomorphism, and, consequently, it is an isomorphism (in the topological sense as well, of course). Therefore

$$DV = (DHN) = (HN)^L = (HN \cap DV)^L = ((HN \cap D)V)^L = (HN \cap D)^L V.$$

It follows at once that $D = (HN \cap D)^L$.

Proof of 5. Let $\mathfrak{P}$ and $\mathfrak{Q}$ denote the Lie algebras of DG and its radical DT respectively. The $\mathfrak{P}/\mathfrak{Q}$ part of the image $\mathrm{Ad}(DT)$ under the adjoint representation is trivial. Since $\mathrm{Ad}\,D$ is fully reducible, there is a complementary subspace to $\mathfrak{Q}$ in $\mathfrak{P}$ which is left fixed under $\mathrm{Ad}\,D$. Let $\mathfrak{z}$ denote the subalgebra generated by this subspace, and let Z denote the corresponding analytic subgroup of DG. Clearly the elements of Z are fixed under inner automorphisms from D, and $DG = ZDT$. Let $\mathfrak{S}$ be a semi-simple algebra occurring in a Levi-decomposition of $\mathfrak{z}$ and let S denote the corresponding analytic group. Since $\mathfrak{P}/\mathfrak{Q} = \mathfrak{z}/(\mathfrak{z} \cap \mathfrak{Q})$ is semi-simple, $\mathfrak{z} = \mathfrak{S} + (\mathfrak{z} \cap \mathfrak{P})$ and $DG = SDT$. Now select a maximal compact subgroup C of S.

We prove that CD is a maximal compact subgroup of DGN. Let R denote the radical of DGN, and λ denote the epimorphism of the semi-direct product $S\cdot R$ onto SR. Then, as in the proof of 3, the kernel of λ is finite, so that a subgroup in SR is compact if and only if its inverse image in $S\cdot R$ is compact. Consequently, to prove that CD is a maximal compact subgroup of SR, it suffices to prove that $C\cdot D$ is a maximal compact subgroup of $S\cdot R$. Let J be a compact subgroup of $S\cdot R$ containing $C\cdot D$. The image of J under the epimorphism $s\cdot r \rightarrow s$ of $S\cdot R$ onto S is a compact subgroup of S containing C. Therefore it coincides with C and $J = C\cdot(J \cap R)$. But $J \cap R$ is a compact subgroup of $R = DTN$. By part 1, $J \cap R = D$, and therefore $J = C\cdot D$. This proves that $C\cdot D$ is maximal compact in $S\cdot R$, and therefore CD is a maximal compact subgroup in DGN. Since $DG \supset CD$, the first assertion in 5. is proved.

In order to prove that $N \cap DG$ is connected, we observe that there is a homeomorphism of $N/(N \cap DG)$ onto DGN/DG. Let K denote CD. Then

$DGN/DG = (DGN/K)/(DG/K)$. Since K is maximal compact in DGN, the space DGN/K is homeomorphic to euclidean space. The natural map of DGN/K onto $(DGN/K)/(DG/K)$ is a continuous and open map with the inverse image of each point connected. Therefore the image $(DGN/K)/(DG/K)$ is simply connected. Therefore

$$N/(N \cap DG) = DGN/DG = (DGN/K)/(DG/K)$$

is simply connected. It follows that $N \cap DG$ is connected. Proof of Lemma 3.3 is now complete.

LEMMA 3.4. *Let ρ be a representation of a group G by automorphisms of a linear space V over a field of characteristic zero. Let M and U be a maximal fully reducible subgroup and the maximum normal subgroup of unipotent elements, respectively, in F, the smallest algebraic group in $GL(V)$ containing $\rho(G)$. Let $\sigma(g)$ denote the image of $\rho(g)$ under the map μ: $mu \rightarrow m$ of MU onto M. Then σ is a representation of G equivalent to ρ'.*

Proof. That σ is a representation of G follows from the fact that $mu \rightarrow m$ is a homomorphism of the algebraic group hull F (see Remark 2.3 above). The set $\sigma(G)$, being in F, keeps invariant any linear subspace of V that is invariant under $\rho(G)$. It suffices, therefore, to verify that if X and Y are linear subspaces invariant under $\rho(G)$ with $X \supset Y$, and if $\rho_{x/y}$, the X/Y part of ρ, is irreducible, then $\rho_{x/y}$ coincides with the X/Y part of σ. In that case $\rho_{x/y}(U) = (1)$; for the subspace of elements in X/Y that are fixed under U must be invariant under G and, therefore, must coincide with X/Y. Consequently $\rho_{x/y}(g) = \rho_{x/y}(g)u_{X/Y} = (\rho(g)u)_{X/Y} = \sigma(g)_{X/Y}$, where $u = \rho(g)^{-1}\sigma(g) \in U$. The proof is now complete.

LEMMA 3.5. *Let G be an analytic group and T its radical. Let H be an analytic subgroup whose Lie algebra is a Cartan subalgebra of the Lie algebra of T, and let D be a compact subgroup of G which lies in the centralizer of H. Let ρ be a representation of G. Then the associated semisimple representation ρ' is equivalent to a representation σ having the same representation space that ρ has and such that* 1) *$\sigma(g) = \rho(g)'$ for all $g \in H$; and* 2) *$\sigma(d) = \rho(d)$ for $d \in D$.*

Proof. The group $\rho(D)$ is compact and therefore fully reducible. Furthermore, $\rho(D)$ lies in the centralizer of $\rho(H)$ and, therefore, in the centralizer of $\rho(H)^*$. Let A be a maximal fully reducible subgroup of $\rho(H)^*$. It is well known, and it is easily seen, that $\rho(D) \cdot A$ is fully reducible. Let M be a maximal fully reducible subgroup of $\rho(G)^*$ containing $\rho(D) \cdot A$, and let U be the maximum normal subgroup of unipotent element in $\rho(G)^*$. Then $\rho(G)^* = MU$ (semi-direct) (Remarks 2.2 and 2.3).

We assert first that A is central in $\rho(H)^*$. For let $\mathscr{C}$ and $\mathscr{B}$ denote the Lie algebras of $\rho(H)$ and $\rho(H)^*$ respectively. We identify these in the usual way with Lie subalgebras of the algebra E all endomorphisms of the underlying linear space. Let $C(x)$ denote the conjugation $y \rightarrow xyx^{-1}$ of E whenever x is an invertible element in E. Since the Lie algebra of H is nilpotent, the same is true of $\mathscr{C}$ and therefore of $\mathscr{B}$. Let $\beta(x)$ denote the restriction of $C(x)$ to $\mathscr{B}$ for $x \in \rho(H)^*$. Clearly β coincides with the adjoint representation of $\rho(H)^*$, and therefore it is unipotent. Hence $\beta(A)$ is a unipotent family. On the other hand, β is a rational representation, and therefore $\beta(A)$ is a fully reducible family. It follows immediately that $\beta(A)$ consists only of the identity element. Thus Ad A is trivial on $\mathscr{B}$, and consequently A commutes with the elements of $\rho(H)^*$. Since $A \subset \rho(H)^*$, A is a commutative fully reducible group. From this it follows that all its elements are fully reducible. Moreover, if $a \in A$ and $u \in \rho(H)^* \cap U$, then $(au)' = a$ since the Jordan product decomposition is unique.

We now define μ to be the epimorphism $mu \rightarrow m$ of $\rho(G)^*$ onto M, and we set $\sigma = \mu \cdot \rho$. Then for $h \in H$, $\sigma(h) = \mu(\rho(h)) = \rho(h)'$, and for $d \in D$, $\sigma(d) = \mu(\rho(d)) = \rho(d)$. Also, σ is equivalent to ρ', by Lemma 3.4. Proof of Lemma 3.5 is now complete.

Note. The proof of Lemma 3.5 establishes the fact that the totality of semi-simple elements in a nilpotent algebraic group B is central in B and therefore coincides with the maximal fully reducible subgroup of B.

4. The first partial extension.

This section and the one following are devoted to a proof of the following extension theorem.

THEOREM 4.1. *Let L be an analytic group, G a closed normal analytic subgroup, and let ρ be a finite dimensional representation of G. Let ρ' denote the semi-simple representation of G associated with ρ, and let N denote the radical of the commutator subgroup L'. In order that the representation ρ can be extended to a finite dimensional representation of L* (see Section 2, Remark 2.7, for definition), *the following three conditions are necessary and sufficient:*

1) *ρ' is trivial on $G \cap N$.*

2) *The representation σ of the analytic group GN defined by $\sigma(gu) = \rho'(g)$* (the existence of σ being asured by Condition 1) *is continuous in the topology of GN relative to L.*

3) *Let P denote the intersection of the kernels of all finite dimensional representations of L. Then* ρ *is trivial on* $P \cap G$.

The necessity of these conditions is fairly clear (see Remark 2.7). We prove sufficiency in two stages. In this section, we show how to extend ρ from G to a certain analytic subgroup F of $\overline{GN}$ that contains a maximal compact subgroup of $\overline{GN}$. In the following section, we apply the results of ERI, to extend the rest of the way to L. The first extension relies heavily on the representation ρ' as described in Lemma 3.5 above.

LEMMA 4.1. *In addition to the assumptions of Theorem* 4.1, *assume that* L *is a linear analytic group. Then there exists a closed connected subgroup* F *of* L *such that* 1) F *contains a maximal compact subgroup of* $\overline{GN}$, $FN = \overline{GN}$ *and* $G \subset F \subset G^*$; 2) ρ *can be extended to a representation* θ *of* F *having the same representation space as* ρ; 3) *The associated semi-simple representaiton* θ' *is trivial on* $N \cap F$.

Proof. We take care to distinguish between the analytic group topology of L and its topology relative to the full linear group. Accordingly, the GN of Lemma 4.1 is hereafter renoted by $(GN)^L$, following the notation of Section 2.

Let T denote the radical of G. Let H be an analytic subgroup of G whose Lie algebra is a Cartan subalgebra of the Lie algebra of T. Let D be a maximal compact subgroup in $(H^* \cap (TN)^L)_1$. By the note following Lemma 3.5, D is central in H^* and, therefore, is in the centralizer of H. Now select the associated semi-simple representation ρ' as in Lemma 3.5 with $D \cap G$ as the "D" of that lemma. By hypothesis 2 of Theorem 4.1, the representation σ is continuous on GN in the topology relative to L. *It follows quite directly that* σ *is the restriction to* GN *of a representation* τ *of* $(GN)^L$. If $d \in D \cap G$ we have $\tau(d) = \sigma(d) = \rho(d)$, by Lemma 3.5. On the semi-direct product $D \cdot G$ we define a map ϕ by the formula $\phi(d \cdot g) = \tau(d)\rho(g)$. The kernel of the epimorphism $d \cdot g \rightarrow dg$ of $D \cdot G$ onto DG consists of all elements $d \cdot d^{-1}$ with $d \in D \cap G$. Thus ϕ maps this kernel into the identity.

We show next that ϕ is a homomorphism. To do so, we define five homomorphisms α, β, $\bar{\beta}$, γ, δ. Let $\mathcal{E}$ and $\mathfrak{F}$ denote the Lie algebras of all endomorphisms on the linear spaces on which G and $\rho(G)$ operate respectively. Let $C(x)$ denote conjugation by x if x is an invertible endomorphism. We identify the Lie algebras of all linear Lie groups with Lie subalgebras of the full linear algebra in the usual way. We shall consistently denote the

Lie algebra of a Lie group by affixing a dot superscript to the symbol for the group. We denote by δ the map which assigns to an automorphism t of any analytic group S, its differential $t^{\cdot}$ at the identity element. The map δ is an isomorphism of $\operatorname{Aut} S$, the automorphism group of S, into $\operatorname{Aut} S^{\cdot}$, the automorphism group of its Lie algebra $S^{\cdot}$. Strictly speaking, δ depends on S but we shall employ the same letter δ for all analytic groups.

The kernel K of ρ is normal in G. By Lemma 3.2, K is normal in G^*. For $g \in G^*$, let $\alpha(g)$ denote the operation of g on G/K that is induced by the conjugation $C(g)$. Clearly $\delta \cdot \alpha(g)$ coincides with the $G^{\cdot}/K^{\cdot}$ part of $C(g)$. Therefore $\delta \cdot \alpha$ is a rational representation.

The map β (resp. $\bar{\beta}$) is the isomorphism between $\operatorname{Aut} G/K$ and $\operatorname{Aut} \rho(G)$ (resp. $\operatorname{Aut} G^{\cdot}/K^{\cdot}$ and $\operatorname{Aut} \rho(G)^{\cdot}$) that is induced by ρ. The map γ is defined for all $y \in \rho(G)^*$ by making $\gamma(y)$ the operation of y on $\rho(G)$ that is induced by $C(y)$. Just as in the case of $\delta \cdot \alpha$, $\delta \cdot \gamma$ is a rational representation of $\rho(G)^*$ in $\operatorname{Aut}(\rho(G))^{\cdot}$. In addition, $\bar{\beta}$ is rational.

We shall prove that $\beta \cdot \alpha(d) = \gamma \cdot \tau(d)$ for all $d \in D$.

$$\begin{tikzcd}
G^* \supset D \arrow[r, "\alpha"] \arrow[d, "\tau"] & \operatorname{Aut} G/K \arrow[r, "\delta"] \arrow[d, "\beta"] & \operatorname{Aut} G^{\cdot}/K^{\cdot} \arrow[d, "\bar{\beta}"] \\
\rho(G)^* \arrow[r, "\gamma"] & \operatorname{Aut} \rho(G) \arrow[r, "\delta"] & \operatorname{Aut} \rho(G)^{\cdot}.
\end{tikzcd}$$

For $d \in HN \cap D$, we have $d = hn$, $h \in H$, $n \in N$, $\tau(d) = \tau(h)\tau(n) = \tau(h) = \rho(h)'$, by Lemma 3.5. Therefore $\delta \cdot \gamma \cdot \tau(d) = \delta \cdot \gamma(\rho(h)') = (\delta \cdot \gamma(\rho(h)))'$, since a rational representation carries the semi-simple part of an endomorphism into the semi-simple part of its image (see Section 2). We observe that $d = h'$. For let A be a maximal fully reducible subgroup in H^*, and let U denote the maximal normal anlaytic subgroup of unipotent elements. Then $H^* = AU$, and $(HN)^* = H^*N = A(UN)$ with $A(UN)$ isomorphic to the semi-direct product $A \cdot (UN)$ (Remarks 2.1 and 2.3). Since A contains all the semi-simple elements of H^* (see note following Lemma 3.5), it follows that $d \in A$ and also $h' \in A$. We have $d = hn = h'(h'^{-1}hn)$, where $h'^{-1}hn \in UN$. From the unique representation of elements in $A \cdot (UN)$, we infer that $d = h'$.

Next observe that ρ is a homomorphism of G, so that by definition of β, $\gamma \cdot \rho = \beta \cdot \alpha$ on G. Also, $\delta \cdot \beta = \bar{\beta} \cdot \delta$. Therefore

$$\begin{aligned}
(\delta \cdot \gamma(\rho(h)))' &= (\delta \cdot \gamma \cdot \rho(h))' = (\delta \cdot \beta \cdot \alpha(h))' = ((\beta \cdot \delta) \cdot \alpha(h))' \\
&= (\bar{\beta} \cdot (\delta \cdot \alpha)(h))' = \bar{\beta}((\delta \cdot \alpha(h))') = \bar{\beta}((\delta \cdot \alpha)(h')) \\
&= \bar{\beta} \cdot \delta \cdot \alpha(h') = \bar{\beta} \cdot \delta \cdot \alpha(d) = \delta \cdot \beta \cdot \alpha(d).
\end{aligned}$$

Therefore $\delta\cdot\gamma\cdot\tau(d)=\delta\cdot\beta\cdot\alpha(d)$ for $d\in HN\cap D$. Since δ is a monomorphism, we get $\gamma\cdot\tau(d)=\beta\cdot\alpha(d)$ for $d\in HN\cap D$. Since $HN\cap D$ is dense in D, we get $\gamma\cdot\tau=\beta\cdot\alpha$ throughout D.

Let $d_1\cdot g_1$ and $d_2\cdot g_2$ be elements of the semi-direct product $D\cdot G$. Then

$$\begin{aligned}\phi(d_1\cdot g_1)\phi(d_2\cdot g_2)&=\tau(d_1)\rho(g_1)\tau(d_2)\rho(g_2)\\&=\tau(d_1)\tau(d_2)(\tau(d_2)^{-1}\rho(g_1)\tau(d_2))\rho(g_2)\\&=\tau(d_1d_2)(\gamma\cdot\tau(d_2)(\rho(g_1)))\rho(g_2)=\tau(d_1d_2)(\beta\cdot\alpha(d_2)(\rho(g_1)))\rho(g_2).\end{aligned}$$

Now by definition of β, $\beta\cdot\alpha(d_2)(\rho(g_1))=\rho(d_2^{-1}g_1d_2)$. Thus

$$\begin{aligned}\phi(d_1\cdot g_1)\phi(d_2\cdot g_1)&=\tau(d_1d_2)\rho(d_2^{-1}g_1d_2)\rho(g_2)\\&=\tau(d_1d_2)\rho(d_2^{-1}g_1d_2g_2)=\phi((d_1\cdot g_1)(d_2\cdot g_2)).\end{aligned}$$

Thus ϕ preserves products and is indeed a homomorphism of the analytic group $D\cdot G$. We have seen that the kernel of ϕ contains the kernel of the epimorphism $D\cdot G\to DG$. Therefore ϕ induces a representation θ of DG, and, obviously, θ is an extension of ρ.

Next we prove that $\theta'(N\cap DG)=1$. By part 5 of Lemma 3.3, $N\cap DG$ is connected. Therefore $N\cap DG$, being a solvable normal analytic subgroup, is in the radical of DG. Hence $N\subset DT$. But $T=HT'$. Thus $N\cap DG\subset DHT'$. Let $n\in N\cap DG$. Then $n=dhu$ with $d\in D$, $h\in H$, and $u\in T'$. We have $1=\tau(n)=\tau(d)\tau(h)\tau(u)=\tau(d)\rho'(h)=\tau(d)\rho(h)'$. Therefore

$$\begin{aligned}\phi(n)&=\phi(d)\phi(h)\phi(u)=\tau(d)\rho(h)\rho(u)\\&=\tau(d)\rho(h)')^{-1}\rho(h)\rho(u)=((\rho(h)')^{-1}\rho(h))\rho(u).\end{aligned}$$

Now by hypothesis 1 of Theorem 4.1, $\rho'(u)=1$, so that $\rho(u)$ is unipotent. Furthermore, $(\rho(h)')^{-1}\rho(h)$ is unipotent by definition of $\rho(h)'$. In addition $(\rho(h)'^{-1})\rho(h)$ and $\rho(h)$ are contained in the algebraic group hull J of the solvable analytic group $\rho(T)$. Since J is solvable and algebraically connected, it follows from Lie's theorem on simultaneous triangularizing of solvable linear Lie algebras that the product of unipotent endomorphisms in J is unipotent. Therefore $\theta(n)=(\rho(h)'^{-1}\rho(h))\rho(u)$ is unipotent for all $n\in N\cap DG$. It follows that θ is unipotent on $N\cap DG$ (Section 2 of ERI). Since $N\cap DG$ is normal in DG, θ' is trivial on $N\cap DG$ (see Section 2 of ERI).

In order to complete the proof of Lemma 4.1, we need only mention that F should be selected as DG.

5. Completion of proof. We proceed under the assumptions of Theorem 4.1. Our first step is to replace L by L/P and to replace ρ by the induced representation of GP/P whose existence is assured by hypothesis 3. After this substitution is made, hypothesis 3 is satisfied trivially. Indeed, the group L is then separated by its finite dimensional representations and, therefore, has a *faithful* finite dimensional representation (Remark 2.5). Consequently, we lose no generality when we assume, in addition to the hypotheses of Theorem 4.1, that L is an analytic *linear* group. We can then apply Lemma 4.1, and assume that the representation ρ has been extended to an analytic subgroup F of L, such that $G \subset F \subset G^*$, $FN = (GN)^L$, and F contains a maximal compact subgroup of $(GN)^L$. We denote the extended representation by ρ also.

We assert that there is a normal series $F_0 = F \subset F_1 \subset \cdots \subset F_r = (GN)^L$ with F_i a closed normal analytic subgroup in F_{i+1}, and F_{i+1}/F_i isomorphic to a 1-dimensional vector group $(i = 1, \cdots, r-1)$. For the commutator subgroup of G^* coincides with the commutator subgroup of G (see [2], p. 173, Th. 13, for the Lie algebra formulation). Therefore $A = (G^* \cap (GN)^L)_1/F$ is abelian. Since F contains a maximal compact subgroup of $(G^* \cap (GN)^L)_1$, the quotient space A is simply connected (see Remark 2.6). A composition series of analytic subgroups for A induces a normal series of analytic subgroups. $F_0 = F \subset F \quad \subset \cdots \subset F_s = (G^* \cap (GN)^L)_1$ with each F_{i+1}/F_i a one dimensional vector group. We next observe that $(G^* \cap (GN)^L)_1$ is a closed normal connected subgroup of $(GN)^L$ and the factor group is

$$FN/(G^* \cap FN)_1 = N/(N \cap (G^* \cap FN)_1),$$

which is solvable. Inasmuch as $(G^* \cap FN)_1$ contains a maximal compact subgroup of FN, the quotient space is simply connected (Remark 2.6). A composition series of analytic subgroups for $FN/(G^* \cap FN)_1$ induces a normal series of analytic subgroups $F_s = (G^* \cap (GN)^L)_1 \subset F_{s+1} \subset \cdots \subset F_r = (GN)^L$, and clearly F_{i+1}/F_i is a one dimensional vector group $(i = s, s+1, \cdots, r-1)$.

Next, we select in each F_{i+1} a one parameter subgroup P_i satisfying a) P_i is not entirely in F_i, and b) $P_i \subset F_{i+1} \cap N$ if $(F_{i+1} \cap N)_1 \neq (F_i \cap N)_1$. Condition a) implies that $P_iF_i = F_{i+1}$. Since $P_i/P_i \cap P_iF_i/F_i = F_{i+1}/F_i$ is simply connected, $P_i \cap F_i$ consists of the identity alone. Therefore the epimorphism of the semi-direct product $P_i \cdot F_i$ onto P_iF_i is an isomorphism. We assert that $N \cap F_{i+1} = (N \cap P_i)(N \cap F_i)$ $(i = 0, \cdots, r-1)$. For $N/(N \cap F_i) = NF_i/F_i = FN/F_i$, and the latter is simply connected since F_i conatins a maximal compact subgroup of FN. Hence $F_i \cap N = (F_i \cap N)_1$, $N \cap P_i = (1)$ or P_i, and $N \cap F_{i+1} = (N \cap P_i)(N \cap F_{i+1})$ by Condition b), $i = 0, \cdots, r-1$. It follows immediately that

$$N = N \cap (GN)^L = (N \cap P_{r-1})(N \cap P_{r-2}) \cdots (N \cap P_0)(N \cap F).$$

Our next step is to apply Remark 2.8 of Sec. 2, in turn, to the semi-direct products $P_0 \cdot F_0, P_1 \cdot F_1, \cdots, P_{r-1} \cdot F_{r-1}$ and thus to extend the representation ρ from $F_0 = F$ to $P_{r-1}F_{r-1} = F_r = (GN)^L$. The construction of the extension provides a representation of $(GN)^L$ unipotent on N (Remark 2.8).

LEMMA 5.1. *Under the hypotheses of Lemma 4.1, there is a normal series of closed analytic subgroups* $L_0 = (GN)^L \subset L_1 \subset \cdots \subset L_j = L$, *and a closed analytic subgroup* $Q_i \subset L_{i+1}$ *such that* $L_{i+1} = Q_i L_i$ *and either* $Q_i \cap L_i$ *contains only the identity element or* Q_i *is compact* $(i = 0, \cdots, j-1)$.

Proof. Let R denote the radical of L and let S be a maximal semi-simple analytic subgroup of L. Then $S \cap R$ is a discrete normal subgroup of S and is therefore central. Since the center of a semi-simple analytic linear group is finite, $S \cap R$ is finite. Therefore the epimorphism $s \cdot r \rightarrow sr$ of the semi-direct product $S \cdot R$ is a finite covering map. It follows easily from this that an analytic subgroup J of L which contains R is closed in L if and only if the connected component $(J \cap S)_1$ is closed. Now $(L_0 R \cap S)_1$ is a normal analytic subgroup of S and is therefore semi-simple. But a semi-simple analytic linear group is closed in the full linear group. Hence $(L_0 R \cap S)_1$ is closed and $L_0 R$ is closed in the analytic group L.

The factor group $L_0 R / L_0$ is a solvable analytic group and therefore has a normal series of closed analytic subgroups whose successive quotients are one-dimensional analytic groups. This normal series provides a normal series of analytic subgroups $L_0 = L \subset L_1 \subset \cdots \subset L_{j-1} = L_0 R$ with L_{i+1}/L_i a one-dimensional analytic group $(i = 0, \cdots, j-2)$. In case L_{i+1}/L_i is simply connected, we select Q_i to be any one parameter group in L_{i+1} that is not entirely in L_i. Then $L_{i+1} = Q_i L_i$, $Q_i \cap L_i$ is discrete in the analytic group Q_i, and $Q_i/(Q_i \cap L_i) = L_{i+1}/L_i$ is simply connected. It follows that $Q_i \cap L_i$ is connected as well as discrete, and therefore it consists only of the identity. Therefore the epimorphism $x \cdot y \rightarrow xy$ of the semi-direct product $Q_i L_i$ onto each such L_{i+1} is an isomorphism and Q_i is closed in L_{i+1}. In the other case that L_{i+1}/L_i is not simply connected, it is compact. Selecting Q_i to be a maximal compact subgroup of L_{i+1}, we obtain $L_{i+1} = Q_i L_i$ (Remark 2.8).

Consider finally the factor group $L/L_0 R = SR/L_0 R = S/(S \cap L_0 R)$. The Lie algebra of $(S \cap L_0 R)_1$ is an ideal of the Lie algebra $S^{\cdot}$ of S. Since $S^{\cdot}$ is a semi-simple Lie algebra, it contains an ideal $Q^{\cdot}$ complementary to the Lie algebra of $(L_0 R \cap S)_1$. Let Q be the analytic subgroup with Lie algebra $Q^{\cdot}$. Then Q is a semi-simple analytic group and is therefore closed. Furthermore, $(Q \cap L_0 R \cap S)_1 = (Q \cap (L_0 R \cap S)_1)_1$ has only zero in its Lie algebra so that $Q \cap L_0R = Q \cap L_0R \cap S$ is a discrete normal subgroup of Q. Hence it is central in Q and finite. Take $Q_j = Q$ and $L_j = L$. The proof of Lemma 5.1 is now complete.

We now conclude the proof of Theorem 4.1. The representation has already been extended to $\overline{GN} = L_0$. Since $N \subset \overline{GN}$, the hypothesis on ρ made in Remark 2.8 is trivially satisfied. Since either Q_i is compact or $Q_i \cap L_i$ contains only the identity, the hypothesis on Q is satisfied. Thus ρ can be extended in j steps from L_0 to L_j via $L_1, L_2, \cdots, L_{j-1}$. The proof of Theorem 4.1 is now complete.

THE INSTITUTE FOR ADVANCED STUDY
AND
THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] C. Chevalley, *Theory of Lie Groups*, Princeton University Press, 1946.

[2] ———, *Theorie des groupes de Lie*, t2, Hermann et C^{ie}, Paris, 1955.

[3] M. Goto, "Faithful representations of Lie groups, II," *Nagoya Mathematical Journal*, vol. 1 (1950), pp. 91-107.

[4] G. Hochschild, "The automorphism group of a Lie group," *Transactions of the American Mathematical Society*, vol. 72 (1952), pp. 209-216.

[5] ——— and G. D. Mostow, "Representations and representative functions of Lie groups," *Annals of Mathematics*, vol. 66 (1957), pp. 495-542.

[6] ——— and ———, "Extensions of representations of Lie groups and Lie algebras, I," *American Journal of Mathematics*, vol. 79 (1957), pp. 924-942.

[7] A. Malcev, "On the theory of Lie groups in the large," *Matematičeskii Sbornik*, T16 (58), N. 2 (1945), pp. 163-190.

[8] G. D. Mostow, "Fully reducible subgroups of alegbraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp. 200-221.

[9] ———, "Factor spaces of solvable groups," *Annals of Mathematics*, vol. 60 (1954), pp. 1-27.

SATAKE'S COMPACTIFICATION OF V_n.*

By WALTER L. BAILY, JR.

In a recent paper [13], Satake has obtained a compactification of the quotient space $V_n = H_n/M_n$, where H_n is the generalized upper half-plane of degree n, i.e., the space of symmetric matrices $Z = X + iY$, where Y is positive definite, and M_n the generalized modular group. This compactification V_n^* is the union $V_n \cup V_{n-1} \cup \cdots \cup V_0$ supplied with a certain topology and analytic structure, concerning which Satake states that it should not be hard to prove that, with this analytic structure, V_n^* is a general analytic space [13]. It is the purpose of this paper to prove that this is indeed the case and that, moreover, V_n^* is isomorphic, as a general analytic space, to a normal projective variety. One of the consequences of our result will be that if f is a meromorphic function in H_n invariant under M_n and if $n \geqq 2$, then f is the quotient of automorphic forms.

In what follows, we refer to the notation of [13]. It is trivial that V_0^* is a general analytic space, and classical that V_1^* is such. If $x \in V_n^*$, we say that V_{n-1}^* has a local basis in V_n^* at x if there exists a finite number of analytic functions (for the given analytic structure) $f_1, \cdots, f_q$ on a neighborhood $\mathfrak{U}$ of x in V_n^* such that $V(f_1, \cdots, f_q) \cap \mathfrak{U} = V_{n-1}^* \cap \mathfrak{U}$, where $V(f_1, \cdots, f_q)$ is the variety of zeros of $f_1, \cdots, f_q$; $f_1, \cdots, f_q$ is called a local basis for V_{n-1}^* at x. We shall first show that if V_{n-1}^* has a local basis at each $x \in V_n^*$, and if V_{n-1}^* is a general analytic space, then V_n^* is a general analytic space.

In what follows, if F is a family or collection of functions defined on some set D, we let $V(F)$ denote the set of common zeros in D of the elements of F. If the elements of F are analytic functions, $V(F)$ is an analytic variety.

To begin with, it is well known that if M_{nx} is the subgroup of M_n leaving fixed $x \in H_n$, then $\text{l.c.m.}_{x \in H_n}(\text{ord}\, M_{nx})$ is a finite positive integer, which we denote by q_n. Secondly, H_n is pseudo-conformally equivalent to a bounded domain D_n in $C^{n(n+1)/2}$, and since the automorphic forms of weight

---

* Received July 22, 1957.

m on H_n with respect to M_n can be identified with the automorphic forms on D_n of a certain weight, we can apply the results of [15], exposé I, on automorphic forms on a bounded domain to obtain immediately

LEMMA I. *There exists a positive integer* m_n *such that the following holds: Let* $x_1, \cdots, x_r \in H_n$ *correspond to* r *distinct points of* H_n/M_n *under the canonical mapping* ϕ_n *of* H_n *onto* H_n/M_n. *Let* a *be a given positive integer. Then for all sufficiently large positive multiples* m *of* m_n, *there exists an automorphic form of weight* m *on* H_n *having prescribed power series developments up to and including the terms of degree* a *at each of the points* $x_1, \cdots, x_r$.

It is clear that we may assume $2 = m_0 \mid m_1 \mid m_2 \mid \cdots$. It is known (Satz 1 of [6]) that for $n > 1$, every automorphic form is bounded on the fundamental domain F_n, i.e., integral. Moreover, if $\Phi_r{}^n$ is the homomorphism defined on p. 278 of [13], and if $\mathfrak{M}_n(m)$ and $\mathfrak{M}_r(m)$ are, respectively, the modules of integral automorphic forms of weight m on $V_n{}^*$ and $V_r{}^*$, then for sufficiently large m, $\Phi_r{}^n : \mathfrak{M}_n(m) \to \mathfrak{M}_r(m)$ is onto by Satz 4 of [8]. For all sufficiently large multiples m of m_n, $V(\mathfrak{M}_n(m))$ is empty; this is trivial for $V_0{}^*$, classical for $V_1{}^*$, and follows for general n by use of an obvious induction using LEMMA I and the fact that $\Phi_{n-1}{}^n$ is onto. In the future we will always assume m_n has been chosen such that $V(\mathfrak{M}_n(m_n))$ is empty.

LEMMA II. *Let* $x \in V_n{}^*$. *Then there exists a neighborhood* $\mathfrak{U}$ *of* x *in* $V_n{}^*$ *such that if* $x_1, x_2 \in V_n \cap \mathfrak{U}$, *there exists a holomorphic function* f *on* $\mathfrak{U}$ *such that* $f(x_1) \neq f(x_2)$. f *may be chosen as a quotient of modular forms.*

Proof. Let $d \in \mathfrak{M}_n(m_n)$ be such that $d(x) \neq 0$. Then let $\mathfrak{U}$ be a neighborhood of x such that $d \neq 0$ on $\mathfrak{U}$. Let $x_1, x_2 \in \mathfrak{U} \cap V_n$. By LEMMA I there exists an automorphic form $g \in \mathfrak{M}_n(m)$, $m_n \mid m$, such that $g(x_1) = 0$, $g(x_2) = 1$. Let $f = g/(d^{m/m_n})$. It is clear that $f(x_1) = 0 \neq f(x_2)$ and that f is holomorphic (in the given analytic structure) on $\mathfrak{U}$.

We shall eventually prove by induction that if $V_{n-1}{}^*$ is a general analytic space, then $V_n{}^*$ is one. Suppose, then, that $V_{n-1}{}^*$ is a general analytic space, let $x \in V_{n-1}{}^*$, and suppose f to be holomorphic on $V_{n-1}{}^*$ in a neighborhood $\mathfrak{U}^*$ of x. We extend f to a holomorphic function on a small neighborhood of x on $V_n{}^*$ as follows: If $Z \in F_n$, let Z_1 be the matrix composed of the first $n-1$ rows and $n-1$ columns of Z; then $Z_1 \in F_{n-1}$, and we define $f(Z) = f(Z_1)$. It is easy to see from Lemma 2′ of [13] that f is a holomorphic function (in the analytic structure prescribed in [13]) in a small neighborhood of x on V_n^*. Since V_{n-1}^* is supposed to be a general analytic space, there exist holomorphic functions $f_{q+1},\cdots,f_p$ in a neighborhood $\mathfrak{U}_1$ of x on V_{n-1}^* such that $V(f_{q+1},\cdots,f_p)=x$, and these functions can be extended, as above, to holomorphic functions $f_{q+1},\cdots,f_p$ on a small neighborhood $\mathfrak{U}_2$ of x on V_n^* such that $V(f_{q+1},\cdots,f_p)\cap V_{n-1}^*=x$.

By definition, a general analytic space is a pair $(V,\mathfrak{A})$, where V is a Hausdorff space and $\mathfrak{A}$ a distinguished subsheaf of the sheaf of germs of continuous, complex-valued functions on V subject to the following condition: If $x\in V$, there exists a neighborhood $\mathfrak{U}$ of x on V, an analytic subvariety W of some open domain in C^m (m depending on x and U), and a homeomorphism h of $\mathfrak{U}$ onto W such that the sheaf, on $\mathfrak{U}$, of germs of continuous functions of the form $f\circ h$, where f is a germ of an analytic function in a neighborhood of some $y\in W$, precisely coincides with $\mathfrak{A}$. $(V,\mathfrak{A})$ is said to be normal if each W is analytically normal at each point. In general, given a Hausdorff space V and a distinguished subsheaf $\mathfrak{A}$ of the sheaf of germs of continuous, complex-valued functions on V, it may be of interest to decide whether $(V,\mathfrak{A})$ (or more loosely speaking, V, when $\mathfrak{A}$ is understood) is a general analytic space; at any rate, the cross-sections of $\mathfrak{A}$ over any open set are to be identified with certain continuous functions, called $\mathfrak{A}$-functions, and if V' is a subset of V, V' is called an $\mathfrak{A}$-variety if for any $x\in V$, there exists a neighborhood $\mathfrak{U}$ of x and a finite number of $\mathfrak{A}$-functions $f_1,\cdots,f_q$ on $\mathfrak{U}$ such that $V(f_1,\cdots,f_q)=V'$, in other words, $f_1,\cdots,f_q$ are a local basis for V' at x. (The terms $\mathfrak{A}$-function and $\mathfrak{A}$-variety are from an unpublished manuscript of H. Grauert and R. Remmert entitled "Bilder und Urbilder analytischer Garben.") Using this terminology, we have

THEOREM 1. *Let V be a Hausdorff space supplied with a distinguished subsheaf $\mathfrak{A}$ of the sheaf of germs of continuous functions. Let V' be an $\mathfrak{A}$-variety on V and let V' be supplied with a distinguished subsheaf $\mathfrak{A}'$ of the sheaf of germs of continuous functions on V'. Suppose that $(V-V',\mathfrak{A}\mid(V-V'))$ is a normal general analytic space and that $(V',\mathfrak{A}')$ is a general analytic space, respectively of dimensions n and m, $m<n$. Suppose, moreover, that the following conditions are satisfied:*

(1) *If V^0 is the set of regular points of $V-V'$, each $x\in V'$ has a neighborhood basis $\{\mathfrak{U}_\alpha\}$ such that each $\mathfrak{U}_\alpha\cap V^0$ is non-empty and connected.*

(2) *If f is a $\mathfrak{A}$-function, $f\mid V'$ is an $\mathfrak{A}'$-function.*

(3) *If f is continuous and if $f\mid(V-V')$ is an $\mathfrak{A}$-function, then f is an $\mathfrak{A}$-function.*

(4) *If* $x \in V'$, *there exists a neighborhood* $\mathfrak{U}$ *of* x *such that* (i) *There exist a finite number of* $\mathfrak{A}$*-functions* $f_{q+1}, \cdots, f_p$ *on* $\mathfrak{U}$ *such that* $V(f_{q+1}, \cdots, f_p) \cap V' = x$, *and* (ii) *If* $x_1, x_2 \in \mathfrak{U} - V'$, $x_1 \neq x_2$, *there exists an* $\mathfrak{A}$*-function* f *on* $\mathfrak{U}$ *such that* $f(x_1) \neq f(x_2)$.

Then $(V, \mathfrak{A})$ *is a normal general analytic space.*

Proof. Let $x \in V'$, let $\mathfrak{U}_3$ be a neighborhood of x satisfying 4(i) and 4(ii). We may assume $\mathfrak{U}_3$ chosen so that there are $\mathfrak{A}$-functions $f_1, \cdots, f_q$ on $\mathfrak{U}_3$ such that $V(f_1, \cdots, f_q) = V'$, let $f_{q+1}, \cdots, f_p$ satisfy 4(i), and let $f_{p+1}, \cdots, f_s$ be arbitrary $\mathfrak{A}$-functions on $\mathfrak{U}_3$. Let $f: \mathfrak{U}_3 \to C^s$ be defined by $f(y) = (f_1(y), \cdots, f_s(y))$. We assume in what follows that all neighborhoods $\mathfrak{U}_3$, $\mathfrak{U}_5$, etc., are such that $\mathfrak{U}_i$ is open and $\mathfrak{U}_i \cap V_n$ is connected, $i = 1, 2, \cdots$. THEOREM 1 is proved by means of two lemmas.

LEMMA III. *There exists a neighborhood* $\mathfrak{U}_7$ *of* x *and an integer* $\beta \geqq 0$ *such that*

(1) $f(\mathfrak{U}_7)$ *is an irreducible analytic variety at* $f(x)$.

(2) $f^{-1}(f(x)) \cap \mathfrak{U}_7 = x$.

(3) $f(V' \cap \mathfrak{U}_7)$ *is a subvariety of* $f(\mathfrak{U}_7)$, *and there exists a proper subvariety* $\mathscr{S}$ *of* $f(\mathfrak{U}_7) - f(V' \cap \mathfrak{U}_7)$ *such that if* $y \in f(\mathfrak{U}_7) - f(V' \cap \mathfrak{U}_7) - \mathscr{S}$, $f^{-1}(y)$ *consists of exactly* β *points, and* f *is biregular at each* $y' \in f^{-1}(y)$.

Proof. In what follows we use a superscript c to denote "closure of." First of all, $V(f_1, \cdots, f_q) \cap \mathfrak{U}_3 = V' \cap \mathfrak{U}_3$ and $V(f_1, \cdots, f_p) \cap \mathfrak{U}_3 = x$. Let $\mathfrak{U}_5$ be a neighborhood of x such that $\mathfrak{U}_5^c \subset \mathfrak{U}_3$. Then there exist neighborhoods $\mathfrak{U}_6$ and $\mathfrak{U}_7$ of x, and a neighborhood N_1 of $f(x)$ such that (a) $\mathfrak{U}_7^c \subset \mathfrak{U}_6$, $\mathfrak{U}_6^c \subset \mathfrak{U}_5$, and (b) $f^{-1}(N_1^c) \cap \mathfrak{U}_5^c \subset \mathfrak{U}_7$. These facts follow easily from the fact that $f^{-1}(f(x)) \cap \mathfrak{U}_3 = x$ and from the continuity of f. Moreover, let $\{\mathfrak{U}_8(\delta)\}$ be a basis of neighborhoods of the set $V' \cap \mathfrak{U}_3$ closed in $\mathfrak{U}_3$. Then for each δ, $f(\mathfrak{U}_5^c - \mathfrak{U}_8(\delta))$ is a compact set not meeting $f(V' \cap \mathfrak{U}_5^c)$ since $V(f_1, \cdots, f_q) \cap \mathfrak{U}_3 = V' \cap \mathfrak{U}_3$. Therefore,

$$\operatorname{dist}(f(\mathfrak{U}_5^c - \mathfrak{U}_8(\delta), f(V' \cap \mathfrak{U}_5^c)) = \sigma > 0.$$

Moreover, since f is continuous, for any neighborhood N_2 of $f(V' \cap \mathfrak{U}_5^c)$, there exists a $\mathfrak{U}_8(\delta)$ such that $f(\mathfrak{U}_8(\delta) \cap \mathfrak{U}_5^c) \cap N_1 \subset N_1 \cap N_2$.

By (b), $f(\mathfrak{U}_7)$ is relatively closed in N_1. Since V' is a general analytic space, and by the choice of $f_1, \cdots, f_s$, we may assume⁽¹⁾ that $\mathfrak{U}_7$ (and correspondingly N_1) is chosen so small that $f(\mathfrak{U}_7 \cap V')$ is an irreducible subvariety $\mathcal{F}$ of dimension $= \dim V'$ of N_1. $N_1 - \mathcal{F}$ is connected. Let $a \in N_1 - \mathcal{F}$. If $a \in N_1 - f(\mathfrak{U}_7)$, there exists a neighborhood of a not meeting $f(\mathfrak{U}_7)$. If $a \in f(\mathfrak{U}_7) - \mathcal{F}$, $f^{-1}(a) \cap (\mathfrak{U}_5 - V')$ is a subvariety $\mathfrak{G}_a$ of $\mathfrak{U}_6$, and there exists a neighborhood $\mathfrak{U}_8(\delta)$ of V' not meeting $f^{-1}(a) \cap \mathfrak{U}_7 = f^{-1}(a) \cap \mathfrak{U}_6$. Therefore $f^{-1}(a) \cap \mathfrak{U}_6 \subset \mathfrak{U}_7 - \mathfrak{U}_8(\delta)$. Thus $f^{-1}(a) \cap \mathfrak{U}_6$ is a *compact*, complex analytic subvariety of $\mathfrak{U}_6 - V'$. Let $y_1, y_2 \in f^{-1}(a) \cap \mathfrak{U}_6$, $y_1 \neq y_2$. Then there exists an $\mathfrak{A}$-function g on $\mathfrak{U}_6$ such that $g(y_1) \neq g(y_2)$, whereas g, being holomorphic on $\mathfrak{U}_6 - V'$, is constant on each component of $f^{-1}(a) \cap \mathfrak{U}_6$. Therefore $f^{-1}(a)$ is a discrete, finite set of points, $a_1, \cdots, a_p$. Let $A_1, \cdots, A_p$ be any neighborhoods of $a_1, \cdots, a_p$ on $V - V'$. Then there exists a neighborhood A of a such that $f^{-1}(A) \cap \mathfrak{U}_6 \subset \cup A_i$; for, otherwise, we could find $b \in \mathfrak{U}_6$, $b \neq a_i$, $i = 1, \cdots, p$, such that $f(b) = a$, which is impossible. Therefore, $A \cap f(\mathfrak{U}_7) \subset f(A_1) \cup \cdots \cup f(A_p)$. We can choose A_i, $i = 1, \cdots, p$, so small that each $f(A_i)$ is an analytic variety at a. Therefore $f(\mathfrak{U}_7)$ is an analytic variety in a neighborhood of a. Therefore $f(\mathfrak{U}_7) - \mathcal{F}$ is a complex analytic subvariety, evidently of dimension $= \dim V$, of $N_1 - \mathcal{F}$. Therefore, since $\mathcal{F}$ is of dimension $= \dim V' < \dim V$, $f(\mathfrak{U}_7)$ is an analytic subvariety of N_1 of dimension $= \dim V$ by a result of Remmert and Stein [7]. We see, moreover, reasoning as above, that if J is the (necessarily proper ⁽¹⁾) subvariety of $\mathfrak{U}_7 - V'$ on which the matrix $(\partial f_l / \partial z_{ij})$ has rank $< \dim V$, then $f(J)$ is a subvariety of $f(\mathfrak{U}_7) - \mathcal{F}$. Let S be the set of singular points of $f(\mathfrak{U}_7)$ and let $S' = (f(\mathfrak{U}_7) - \mathcal{F}) \cap S$. $\dim S' < \dim f(\mathfrak{U}_7)$. Therefore $f^{-1}(S')$ is a proper subvariety of $\mathfrak{U}_7 - V'$. Therefore $\mathfrak{U}_7 - V' - f^{-1}(S') - J$ is connected and everywhere dense, however small $\mathfrak{U}_7$ may be chosen, and consequently $f(\mathfrak{U}_7 - V' - f^{-1}(S') - J)$ is a connected, dense set of regular points. Hence $f(\mathfrak{U}_7)$ is irreducible at $f(x)$. Let $a \in (f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S') \cap N_1$, $f^{-1}(a) \cap \mathfrak{U}_6 = f^{-1}(a) \cap \mathfrak{U}_7 = a_1, \cdots, a_\beta$. Then for every point a' near a, $f^{-1}(a') \cap \mathfrak{U}_6 = f^{-1}(a') \cap \mathfrak{U}_7 = a'_1, \cdots, a'_\beta$. Let $A(\beta)$ be the subset of $(f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S') \cap N_1$ such that for $a \in A(\beta)$, $f^{-1}(a) \cap \mathfrak{U}_6 = f^{-1}(a) \cap \mathfrak{U}_7$ consists of just β points. The interior of $A(\beta)$, $\operatorname{Int} A(\beta)$, is not empty. Let $b \in (f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S') \cap N_1 \cap (\operatorname{Int} A(\beta))^c$. Let $b_1, \cdots, b_k = f^{-1}(b) \cap \mathfrak{U}_6$. Since $b \notin f(J)$, there exist neighborhoods $B_1, \cdots, B_k$ of

---

(1) Let W be a purely k-dimensional general analytic space and let $f: W \to C^m$ be a mapping whose coordinates $f_1, \cdots, f_m$ are analytic functions on W. If $f^{-1}(x)$ is discrete

---

for each $x \in f(W)$, we say f is a light analytic map; in this case, it follows immediately from Theorems 5 and 6, exposé XIV of [14], that for each $x^* \in W$, there exists a neighborhood $\mathfrak{U}$ of x^* such that $f(\mathfrak{U})$ is an analytic variety of pure dimension k at $f(x^*)$. Moreover, if f is light analytic and if W^0 is the set of regular points of W, it is easy to show by a simple dimension argument that the subset J of W^0, on which the Jacobian matrix of the mapping f has rank $< k$, is a proper subvariety of W^0.

$b_1, \cdots, b_k$ which are pair-wise disjoint and such that f is one-to-one on each B_i. Since, moreover, $b \notin S'$, $f(B_i)$ contains a neighborhood of b on $f(\mathfrak{U}_7)$, $i = 1, \cdots, k$. Finally, $b \in (\operatorname{Int} A(\beta))^c$. Therefore $k \leqq \beta$. Suppose $k < \beta$. Let $a^{(j)} \to b$, $f^{-1}(a^{(j)}) = a_1^{(j)}, \cdots, a_\beta^{(j)}$. Then for some i, there exists a subsequence of $a_i^{(j)}$ having for limit $\alpha \neq b_1, \cdots, b_k$. $\alpha \in \mathfrak{U}_6$, and, by continuity, $f(\alpha) = b$, which is impossible. Therefore $k = \beta$. Hence $(\operatorname{Int} A(\beta))^c$ is open in the connected set $(f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S') \cap N_1$. Therefore $A(\beta) = (f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S') \cap N_1$. We let $\mathcal{S} = f(J) \cup S'$. This completes the proof of LEMMA III.[2]

LEMMA IV. *For suitable choice of* $f_{p+1}, \cdots, f_s$ *(s sufficiently large),* β *(of* LEMMA III*)* $= 1$.

Proof. Suppose $f_{p+1}, \cdots, f_s$ are such that β is minimal. Let $y \in f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S$, and suppose that $\mathfrak{U}_7 \cap f^{-1}(y) = y_1, \cdots, y_\beta$, $\beta > 1$, $y_1 \neq y_2$. Let g be an $\mathfrak{A}$-function on $\mathfrak{U}_8$ such that $g(y_1) \neq g(y_2)$. If $\zeta \in f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S$, let $f^{-1}(\zeta) = \zeta_1, \cdots, \zeta_\beta$; let $\mathfrak{N}$ be a neighborhood of ζ and $\mathfrak{N}_i$ a neighborhood of ζ_i, $i = 1, \cdots, \beta$, such that f is a biregular mapping of $\mathfrak{N}_i$ onto $\mathfrak{N}$. Let $g_{\zeta i}$ be defined on $\mathfrak{N}$ by $g_{\zeta i}(\xi) = g((f \mid \mathfrak{N}_i)^{-1}(\xi))$ for $\xi \in \mathfrak{N}$. Let $I(\mathfrak{N}) = \{\xi \mid \xi \in \mathfrak{N}, g_{\zeta 1}(\xi) = \cdots = g_{\zeta\beta}(\xi)\}$. $I(\mathfrak{N})$ is the subset of $\mathfrak{N}$ consisting of those $\xi \in \mathfrak{N}$ such that g has the same value at each point of $f^{-1}(\xi)$, and $I(\mathfrak{N})$ is a subvariety of $\mathfrak{N}$. Therefore if $\{\mathfrak{N}^{(\alpha)}\}$ is a covering of $f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S$ by neighborhoods of the above type, $I = \bigcup_\alpha I(\mathfrak{N}^{(\alpha)})$ is a subvariety of $f(\mathfrak{U}_7) - \mathcal{F} - f(J) - S$. It is a proper subvariety since $y \notin I$. Therefore $f^{-1}(I) = I^*$ is a proper subvariety of $\mathfrak{U}_7 - V' - J - f^{-1}(S)$, and the latter is an everywhere dense open subset of $\mathfrak{U}_7$. Define $f' : \mathfrak{U}_7 \to C^{s+1}$ by $f'(y) = (f_1(y), \cdots, f_s(y), g(y))$. By LEMMA III, there exists a neighborhood $\mathfrak{U}'_7$ of x such that $f'(\mathfrak{U}'_7)$ is an irreducible variety at $f'(x)$ and such that $f'(\mathfrak{U}'_7)$ is an irreducible variety at $f'(x)$ and such that if ζ belongs to an everywhere dense open subset of $f'(\mathfrak{U}'_7)$, then $f'^{-1}(\zeta) = \zeta_1, \cdots, \zeta_{\beta_1}$, and by assumption, $\beta_1 \geqq \beta$. On the other hand, if ξ belongs to the everywhere dense open subset $f'(\mathfrak{U}_7 - V' - J - f^{-1}(S) - I^*)$, $f'^{-1}(\xi)$ consists of at most $\beta - 1$ points, which is a contradiction. This establishes the lemma. (Note that since f'^{-1} of any point is discrete,

$$\dim f'(I^*) = \dim I^* < \dim V = \dim f'(\mathfrak{U}'_7).)$$

---

[2] It is easy to see that at this point, having proved LEMMA III, we could apply Theorem 3 of [4] to obtain immediately that V is a normal general analytic space. However, we give here, for the sake of completeness, a relatively simple, elementary proof, independent of [4].

Now let $f_{p+1}, \cdots, f_s$ be chosen such that β (of LEMMA III) $= 1$. Let $f(\mathfrak{U}_7) \cap N_1 = W$ and let $W^{\#}$ be the canonical normal model(3) of W. We define a mapping $f^{\#}$ of $f^{-1}(V) \cap \mathfrak{U}_7$ into $W^{\#}$. Let $b \in W$ and let $f^{-1}(b) = b_1, \cdots, b_\gamma$. By LEMMA III, there exists a neighborhood B_i of b_i, $i = 1, \cdots, \gamma$, such that $B_i \subset \mathfrak{U}_7$ and such that $f(B_i)$ defines an irreducible germ of a variety $f(B_i)_b$ at b. Since f is one-to-one on an everywhere dense subset of $\mathfrak{U}_7$, $i \neq j$ implies that $f(B_i)$ and $f(B_j)$ define distinct irreducible germs at b. The points of $W^{\#}$ are pairs consisting of a point of W together with an irreducible branch of W at that point. We define $f^{\#}(b_i)$ to be $(b, f(B_i)_b)$. It is clear that $f^{\#}$ is one-to-one and continuous. If p is the canonical mapping of $W^{\#}$ onto W, p is continuous and $pf^{\#} = f$. If K is a compact subset of $W^{\#}$, $f^{\#-1}(K) = f^{-1}p(K)$. Since f is proper, it follows that $f^{\#}$ is, and therefore $f^{\#}$ is a homeomorphism. Let $\mathscr{B}$ be the subvariety of W defined by: $\mathscr{B} = \{x \mid x \in W,\ W \text{ not normal at } x \text{ or } x \in f(V')\}$. $\dim \mathscr{B} < \dim W$, and since p conserves dimensions, $p^{-1}(\mathscr{B})$ is a proper subvariety $\mathscr{B}^{\#}$ of $W^{\#}$. If g is an $\mathfrak{A}$-function on an open subset $\mathfrak{U}$ of $f^{-1}(W) \cap \mathfrak{U}_7$, $g \circ f^{\#-1}$ is continuous on $f^{\#}(\mathfrak{U})$, and holomorphic outside $\mathscr{B}^{\#}$; for if $a \in V - V'$, $f^{\#}$ is an analytic isomorphism of a neighborhood A of a with the normal model of $f(A)$, which is just $p^{-1}(f(A))$. Therefore $g \circ f^{\#-1}$ is holomorphic on all of $f^{\#}(\mathfrak{U})$. Conversely, if g' is holomorphic on an open subset $\mathfrak{U}^{\#}$ of $W^{\#}$, $g' \circ f^{\#}$ is an $\mathfrak{A}$-function on $f^{\#-1}(\mathfrak{U}^{\#})$ outside V' for just the same reason. Therefore, by (3) of Theorem 1, $g' \circ f^{\#}$ is an $\mathfrak{A}$-function on all of $f^{\#-1}(\mathfrak{U}^{\#})$. Consequently, $f^{\#}$ is an analytic isomorphism of $f^{-1}(N_1) \cap \mathfrak{U}_7$ onto $W^{\#}$. Thus there is a neighborhood of x analytically isomorphic to a normal general analytic space. The proof of Theorem 1 is complete.

THEOREM 2. *If V_{n-1}^* has a local basis at each point of V_n^*, and if V_{n-1}^* is a general analytic space, then V_n^* is a normal general analytic space.*

Proof. Let $V = V_n^*$, $V' = V_{n-1}^*$, each supplied with the analytic structure descirbed in [13]. V_{n-1}^* is an $\mathfrak{A}$-variety, since, by hypothesis, V_{n-1}^* has a local basis at each $x \in V_n^*$. We know that $V_n^* - V_{n-1}^* = V_n = H_n/M_n$ is a normal general analytic space ([15], exposé XII), V_{n-1}^* is a general analytic space by hypothesis, while $\dim V_{n-1} = \frac{1}{2}n(n-1) < \frac{1}{2}n(n+1) = \dim V_n$, if $n > 0$. (1) is satisfied by virtue of the topology with which V_n^* is supplied (see [13], pp. 266-273), and (2) and (3) are satisfied by virtue of the definition of the analytic structure for V_n^* and by the properties of the operator Φ described on pp. 278-280 of [13].(4) (4i) is satisfied by the remarks following the proof of LEMMA II, while (4ii) is satisfied by LEMMA II itself. This completes the proof.

---

(3) By the canonical normal model of a complex analytic variety W, we mean the space of parameters $\mathfrak{F}_W$ as defined in no. 9, exposé XIV of [14], supplied with the analytic structure described in no. 10 (loc. cit.). That $\mathfrak{F}_W$ is isomorphic to a general analytic space is proved in exposés X and XI of [15], the proof depending on the coherence of the sheaf $\bar{A}(E)$ (exposé X, [15]). The coherence of $\bar{A}(E)$ was originally demonstrated in [10].

It now remains to be proved that V_{n-1}^* has a local basis at each $x \in V_n^*$. It is trivial that V_{n-1}^* has a local basis at each $x \in V_n$. We now proceed, by a series of lemmas, to show that V_{n-1}^* has a local basis in V_n^* at each $x \in V_{n-1}^*$. Let $x \in V_{n-1}^* = V_{n-1} \cup \cdots \cup V_0$ and suppose $x \in V_\rho$, $1 \leqq \rho \leqq n-1$. Let x be the canonical image in V_ρ of $Z_1^0 \in F_\rho$. Z_1^0 is a $\rho \times \rho$ matrix, reduced in the sense of Siegel, whose imaginary part Y_1^0 is reduced in the sense of Minkowski. Let G_0 be the finite subgroup of M_ρ leaving Z_1^0 fixed. Let D_0 be the set of $\rho \times (n-\rho)$ matrices Z_{12} such that each of the entries of Y_{12} is less in absolute value than A, where A is a suitable large positive number greater than the ρ-th diagonal element of Y_1^0, and such that the real part of each entry of Z_{12} is between $-L$ and $+L$, L being a suitable large positive number $\geqq 1$. Then D_0 is a bounded and therefore relatively compact subset of $C^{\rho(n-\rho)}$. It is clear that if

$$\begin{pmatrix} Z_1^0 & Z_{12} \\ {}^tZ_{12} & Z_2 \end{pmatrix} \in F_n, \text{ where } Z_2 \text{ is } (n-\rho)\times(n-\rho),$$

then $Z_{12} \in D_0$. As in [13] we shall omit ${}^tZ_{12}$ wherever it is redundant.

If T_2 is a positive definite $(n-\rho)\times(n-\rho)$ integral matrix and if T_{12} is a rational multiple of T_2 ([13], p. 275), we let

$$\theta_{T_2,T_{12}}(Z_1, Z_{12}) = \epsilon({}^tT_{12}Z_{12}) \sum_{U_{12}} \epsilon(Z_1(T_2[{}^tU_{12}]) + {}^tU_{12}(Z_1T_{12} + 2Z_{12}T_2)),$$

U_{12} running over all $\rho \times (n-\rho)$ integral matrices, where now, as in the future, $\epsilon(\ ) = e^{2\pi i S\rho(\ )}$, and $\epsilon'(\ ) = e^{-\pi S\rho(\ )}$. Let E be the identity matrix (of any dimension). Then if $T_2 = mE$, where m is a positive integer, if T_{12} is a rational multiple of mE whose entries are even integers (briefly, an even rational multiple of mE), and if the columns of T_{12} are $2\tau_1, \cdots, 2\tau_{n-\rho}$, we have

---

(4) In fact, it is evident from Lemma 1 of [13] that if $x \in V_n^*$, there is a basis of neighborhoods $\{\mathfrak{U}_a\}$ of x such that each of the sets $\mathfrak{U}_a \cap V_n$ is connected; moreover, it is clear from the properties of the operator Φ that if f is continuous on $\mathfrak{U}_a$ and analytic on $\mathfrak{U}_a \cap V_n$, then f is analytic on $\mathfrak{U}_a$ by Satake's definition, as we see from Theorem 3 of [13].

$$\theta_{mE,T_{12}}(Z_1,Z_{12}) = \Big(\prod_{i=1}^{n-\rho} \Theta_m[\tau_i](z^i;Z_1)\Big)\mathcal{E}(Z_1,Z_{12}),$$

where z^i is the i-th column of Z_{12} and where $\mathcal{E}$ is a non-vanishing exponential factor. It is known ([2], pp. 158 ff.) that for sufficiently large m, $\Theta_m[\tau_i](z^i;Z_1^0)$ have no common zeros as τ_i runs over all integral ρ-vectors, and since $\tau_1,\cdots,\tau_{n-\rho}$ are independent, $\theta_{mE,T_{12}}(Z_1^0,Z_{12})$ have no common zeros (in Z_{12}) as T_{12} runs over all even rational multiples of mE. Fix m subject to this condition. Then by continuity we can find a connected, open neighborhood $\mathfrak{U}_0$ of Z_1^0 in H_ρ such that:

(1) $\mathfrak{U}_0$ is stable under G_0 and $g\mathfrak{U}_0 \cap \mathfrak{U}_0$ is empty if $g \in M_\rho - G_0$.

(2) $Z_1 \in \mathfrak{U}_0, \begin{pmatrix} Z_1 & Z_{12} \\ & Z_2 \end{pmatrix} \in F_n \Rightarrow Z_{12} \in D_0$.

(3) $Z_1 \in \mathfrak{U}_0 \Rightarrow \theta_{mE,T_{12}}(Z_1,Z_{12})$ have no common zeros as T_{12} runs over all even rational multiples of mE.

(4) $\mathfrak{U}_0$ is bounded.

Let N_ρ be $\mathfrak{N}$ as defined on p. 270 of [13] with $r=\rho$. Then G_0 is naturally identifiable with a subgroup G_0' of M_n ($G_0' \subset M_\rho^{(n)}$ in Satake's notation), $\mathfrak{G} = G_0' \cdot N_\rho$ is a subgroup of M_n, and N_ρ is a *normal* subgroup of $G_0' \cdot N_\rho$. It is clear that we may assume of $\mathfrak{U}_0$ by appropriate choice of A and L to begin with that

(5) If $Z_1 \in \mathfrak{U}_0$, $Z = \begin{pmatrix} Z_1 & Z_{12} \\ & Z_2 \end{pmatrix} \in F_n$, $g \in G_0'$, and if $Z' = gZ$, then $Z_{12}' \in D_0$.

Let $W' = \mathfrak{U}_0 \times D_0$. By Lemma 2 of [13], there exists a real positive definite, symmetric, $(n-\rho)\times(n-\rho)$ matrix Y_2^0 such that if $Y_2 > Y_2^0$, and if $Z = \begin{pmatrix} Z_1 & Z_{12} \\ & Z_2 \end{pmatrix}$, where $(Z_1,Z_{12}) \in W'$, then $\sigma(Z) \in \tilde{V}^{(n)}(\mathfrak{U}_0,K)$ for some $\sigma \in \mathfrak{G}$, where K is a fixed, sufficiently large positive number. Let

$$\mathcal{U}(Y_2^0) = \{Z = \begin{pmatrix} Z_1 & Z_{12} \\ & Z_2 \end{pmatrix} \mid (Z_1,Z_{12}) \in \mathfrak{U}_0 \times D_0, Y_2 > Y_2^0\}.$$

Let

$$\theta_{m,T_{12}}{}^{k}(Z_1,Z_{12}) = \sum_{g \in G_0'} \theta_{mE,T_{12}}(Z_1{}^g,Z_{12}{}^g)^k \epsilon(mk(Z_2{}^g - Z_2)),$$

where if $Z = \begin{pmatrix} Z_1 & Z_{12} \\ & Z_2 \end{pmatrix}$, then $gZ = \begin{pmatrix} Z_1{}^g & Z_{12}{}^g \\ & Z_2{}^g \end{pmatrix}$, and where $1 \leqq k \leqq \operatorname{ord} G_0'$. The legitimacy of this definition, as well as the fact that $\theta_{m,T_{12}}{}^k$ is bounded on W' follow from (20) of [13].

Lemma V. *The functions* $\sum_{j=1}^{r} z_j^k$, $k = 1, \cdots, r$, *have no common zero other than* $z_1 = \cdots = z_r = 0$.

Proof. This is immediate since $z_1, \cdots, z_r$ are integral over the polynomial ring generated by $\sum_{j=1}^{r} z_j^k$, $k = 1, \cdots, r$.

In what follows, let $\eta(r)$ be the positive minimum of $\max_{1 \leqq k \leqq r} |\sum_{j=1}^{r} z_j^k|$ on the compact set $\max |z_j| = 1$. Then if $a > 1$, the positive minimum of $\max_{1 \leqq k \leqq r} |\sum_{j=1}^{r} z_j^k|$ on the compact set $\max |z_j| = a$ is $\geqq a\eta(r)$.

The following lemma, while practically trivial in content, serves to point up the main idea of our approach in what follows.

Lemma VI. *Let* $\{f_\mu\}$ *be a sequence of complex-valued functions on a point set* D *such that* $\sum f_\mu$ *converges absolutely at each point of* D, *and suppose there exists an integer* $C > 0$ *and a finite number of subsets* $D_1, \cdots, D_A$ *of* D *such that*

(i) $D = \bigcup_{a=1}^{A} D_a$.

(ii) *For each* $a = 1, \cdots, A$, *there exist indices* $m_1, \cdots, m_{p_a} < C$ *such that* $V(\{f_{m_k}\}_{k=1,\cdots,p_a}) \cap D_a$ *is empty, and if* $x \in D_a$ *and* $f_{m_k}(x) \neq 0$, *then* $\sum_{\mu > C} |(f_\mu(x)/f_{m_k}(x))^l| \leqq \frac{1}{2}\eta(C)$, $l = 1, \cdots, C$. *Then* $V(\{\sum_\mu f_\mu{}^l\}_{l=1,\cdots,C})$ *is empty.*

Proof. Let $x \in D$. Then $x \in D_a$ for some $a = 1, \cdots, A$. Suppose $f_{m_k}(x) \neq 0$. Choose l, $1 \leqq l \leqq C$, such that $|\sum_{\mu \leqq C} (f_\mu(x)/f_{m_k}(x))^l| \geqq \eta(C)$. It is clear that $|\sum_\mu (f_\mu(x)/f_{m_k}(x))^l| \geqq \eta(C) - \frac{1}{2}\eta(C) = \frac{1}{2}\eta(C) \neq 0$. q. e. d.

Lemma VII. *There exist a finite number of* $r \times r$ *unimodular matrices* $U_1, \cdots, U_{A_r}$ *such that for any reduced (semi-definite or positive definite)* $r \times r$ *matrix* Y, *there is an integer* a, $1 \leqq a \leqq A_r$, *such that* $\operatorname{Sp} Y[U_a] \leqq \operatorname{Sp} Y[U]$ *for all* $r \times r$ *unimodular* U.

Proof. If U_a is any unimodular matrix, the set

$$D_{U_a} = \{Y \mid \operatorname{Sp} Y[U_a] \leqq \operatorname{Sp} Y[U], \text{ all unimodular } U\}$$

is evidently closed (and convex). Hence it suffices to prove the lemma for reduced $Y > 0$. We recall ([16], p. 629 and pp. 642-643) the following facts which hold for any reduced $r \times r$ matrix Y and any semidefinite $r \times r$ matrix T:

(1) $\operatorname{Sp}(YT) = \operatorname{Sp}(TY) \geqq \lambda(r) \sum t_{ii} y_{ii}$, $\lambda(r)$ being a positive number depending only on r, and t_{ii}, y_{ii} being respectively the diagonal elements of T, Y.

(2) $\operatorname{Sp} Y \leqq r y_{rr}$.

(3) $y_{ii} \leqq y_{i+1,i+1}$, $|y_{ij}| = |y_{ji}| \leqq \frac{1}{2} y_{ii}$.

If U_a is any unimodular matrix, denote by $U_a^{(k)}$ the $k \times r$ submatrix of U_a consisting of the last k rows of U_a. We say that U_a is minimizing for Y if $Y \in D_{U_a}$. It is clear that there exist minimizing U_a for any positive semidefinite Y. Let L_k be the assertion that there exist at most finitely many $U_a^{(k)}$ such that U_a is minimizing for some positive definite reduced Y. We shall prove

(a) L_1.

(b) L_k implies L_{k+1}.

Since L_r implies LEMMA VII, this will complete the proof.

Proof of (a). If $U = (u_{ij})$, it is clear from (1) that

$$\operatorname{Sp} Y[U] \geqq \lambda(r) \sum_i y_{ii} \left(\sum_j u_{ij}^2\right) \geqq \lambda(r) y_{rr} \sum_j u_{rj}^2.$$

Since by (2), $\operatorname{Sp} Y \leqq r y_{rr}$, it follows that U can be minimizing for Y only if $\lambda(r) \sum_j u_{rj}^2 \leqq r$, from which L_1 follows.

Proof of (b). Suppose L_k to be true but L_{k+1} false. Then there exists a sequence of $r \times r$ unimodular matrices $\{U_a\}$ and a sequence $\{Y_a\}$ of reduced $Y_a > 0$ such that U_a is minimizing for Y_a and such that $\sum_j (u_{r-k,j}^a)^2 \rightarrow +\infty$, where $U_a = (u_{ij}^a)$. Since there are only a finite number of possibilities for $U_a^{(k)}$, we may assume $U_a^{(k)}$ to be the same for each U_a. Let U^* be an integral $(r-k) \times r$ matrix such that $U_0 = \begin{pmatrix} U^* \\ U_a^{(k)} \end{pmatrix}$ is unimodular. We let U_a^* denote the $(r-k) \times r$ matrix composed of the first $r-k$ rows of U_a, $Y_a = (y_{ij}^a)$, and write $Y_a = \begin{pmatrix} Y_1^a & Y_{12}^a \\ {}^tY_{12}^a & Y_2^a \end{pmatrix}$, Y_2^a being $k \times k$. Then

$$\operatorname{Sp} Y_a[U_a] = \operatorname{Sp} Y_1^a[U_a^*] + 2 \operatorname{Sp} {}^tU_a^* Y_{12}^a U_a^{(k)} + \operatorname{Sp} Y_2^a[U_a^{(k)}].$$

Using (1), (3), and the fact that $U_a^{(k)}$ is fixed, we easily obtain

$$\begin{aligned}\mathrm{Sp}\, Y_a[U_a] &\geqq c \cdot Sp\, Y_1^a[U_a^*] + \mathrm{Sp}\, Y_2^a[U_a^{(k)}] \\ &\geqq c \cdot \sum_j (u_{r-k,j}^a)^2 \cdot y_{r-k,r-k}^a + \mathrm{Sp}\, Y_2^a[U_a^{(k)}],\end{aligned}$$

$c > 0$ being a constant independent of a. On the other hand, using (3), it is clear that

$$\mathrm{Sp}\, Y_a[U_0] \leqq C y_{r-k,r-k}^a + \mathrm{Sp}\, Y_2^a[U_a^{(k)}],$$

$C > 0$ being a constant independent of a. Since U_a is minimizing for Y_a, we must therefore have

$$C y_{r-k,r-k}^a \geqq c \sum_j (u_{r-k,j}^a)^2 \cdot y_{r-k,r-k}^a,$$

and since $Y_a > 0$, we must have $y_{r-k,r-k}^a > 0$; but then the above equation is in evident contradiction to $\sum_j (u_{r-k,j}^a)^2 \to +\infty$. Hence (b) and therefore LEMMA VII is proved.

LEMMA VIII. *There is a finite set* $S(n)$ *of unimodular matrices, a positive definite matrix* Y_0, *and a positive constant* m *such that if* Y *is any reduced* $n \times n$ *matrix*, $Y > kY_0$ $(k \geqq 1)$, *then there exists* U_a, $1 \leqq a \leqq A_n$, *such that* $\mathrm{Sp}(Y[U] - Y[U_a] - mk\,{}^tUU) > 0$, *for any unimodular* $U \notin S$.

Proof. By the reduction theory of Minkowski [9], pp. 68-70, the reduced forms constitute a convex cone with vertex at the origin, bounded by a finite number of plane faces, and therefore having a finite number of 1-dimensional edges which span the interior of the cone. Thus there exist a finite number of reduced $n \times n$ matrices $Y_1, \cdots, Y_s$ such that if Y is a reduced $n \times n$ matrix, Y can be written in the (not generally unique) form $Y = \sum_{i=1}^{s} a_i Y_i$, $a_i \geqq 0$. Let $Y_1, \cdots, Y_p$ be positive definite and $Y_{p+1}, \cdots, Y_s$ be semi-definite, but *not* positive definite. Let $Y' = \sum_{i>p} a_i Y_i$. Then Y' is reduced. Choose a, $1 \leqq a \leqq A_n$, such that U_a is minimizing for Y'. Then $\mathrm{Sp}(Y'[U] - Y'[U_a]) \geqq 0$ for all unimodular U. It is evident that there is a finite set S of $n \times n$ matrices such that if U is unimodular, $U \notin S$, then

$$\mathrm{Sp}(Y_i[U] - Y_i[U_a]) > \alpha \cdot \mathrm{Sp}({}^tUU),\ i = 1, \cdots, p,\quad a = 1, \cdots, A_n,$$

α being a fixed positive number. Let Y be a positive reduced matrix, $Y > cE$, $c > 0$. Then $Y = \sum_{i=1}^{p} a_i Y_i + Y'$, $a_i \geqq 0$, $Y' \geqq 0$, Y' *not* positive definite. Let

δ be the biggest diagonal entry of any Y_i, $i = 1, \cdots, p$. Since $Y > cE$, we have $a_{i'} > c/p\delta$ for some i', $1 \leqq i' \leqq p$. Then if $U \notin S$,

$$\begin{aligned} \mathrm{Sp}\{Y[U] - Y[U_a]\} &= \sum_{i=1}^{p} a_i \, \mathrm{Sp}\{Y_i[U] - Y_i[U_a]\} + \mathrm{Sp}\{Y'[U] - Y'[U_a]\} \\ &\geqq \sum_{i=1}^{p} a_i \, \mathrm{Sp}\{Y_i[U] - Y_i[U_a]\} \geqq \sum_{i=1}^{p} a_i \alpha \cdot Sp({}^tUU) \\ &\geqq (\alpha c/p\delta) \, \mathrm{Sp}({}^tUU). \end{aligned}$$

So we can take $Y_0 = E$, $m = \alpha/p\delta$, $c = k$.

q. e. d.

Let κ be the minimum for $(Z_1, Z_{12}) \in \mathrm{clos}(\mathfrak{U}_0 \times D_0)$ and $a = 1, \cdots, A_{n-\rho}$ of the quantity

$$\max_{k, T_{12}} | \theta_{m, T_{12}}{}^k (Z_1, Z_{12} U_a) |,$$

where $k = 1, \cdots, \mathrm{ord}\, G_0'$, and where T_{12} runs over all even rational multiples of mE. $\kappa > 0$ by Lemma V applied to

$$\theta_{m, T_{12}}{}^1 (Z_1, Z_{12} U_a), \cdots, \theta_{m, T_{12}}{}^{\mathrm{ord}\, G_0'} (Z_1, Z_{12} U_a)$$

for each a. Let

$$\Phi_{m, T_{12}}{}^k (Z) = \sum_{U_2} \theta_{m, T_{12}}{}^k (Z_1, Z_{12} U_2) \epsilon\, (mk U_2 {}^t U_2 Z_2)$$

and

$$\Phi_{m, T_{12}}{}^{kl} (Z) = \sum_{U_2} \theta_{m, T_{12}}{}^k (Z_1, Z_{12} U_2)\, {}^l \epsilon (mkl U_2 {}^t U_2 Z_2),$$

where U_2 runs over all non-associate, unimodular $(n - \rho) \times (n - \rho)$ matrices, and $1 \leqq l \leqq C$, C being the number of elements in the set $S(n - \rho)$ of Lemma VIII. In legitimatizing the above constructions, we let G_{12} be the subgroup of N_ρ such that $U_{12} = S_{12} = 0$, and G_2, the subgroup of N_ρ such that $U_2 = E$, and then note that G_2 is a normal subgroup of $G_0' \cdot N_\rho$, G_{12} is stable under the inner automorphisms of $G_0' \cdot N_\rho$ induced by elements of G_0', and, as previously stated, N_ρ is a normal subgroup of $G_0' \cdot N_\rho$; then each $\Phi_{m, T_{12}}{}^{kl}$ is defined in the form

$$\Phi(Z) = \sum_{\sigma \in G_{12} \bmod S_2} \Big(\sum_{g \in G_0'} f(g\sigma Z)^k \Big)^l,$$

where f is invariant under G_2, and $\sigma \in G_{12} \bmod S_2$ means that for each coset of the subgroup of G_{12} for which $S_1 = S_{12} = 0$, and $U = E$, we choose a coset representative σ; from this, it is evident that Φ is invariant under $G_0' \cdot N$. That the above series converge uniformly for $Y_2 \gg 0$ follows easily from Lemma VIII and the fact that $\mathfrak{U}_0 \times D_0$ is a bounded set.

Denote by D_{U_a}' the subset of $F_{n-\rho}$ consisting of those $Z_2 = X_2 + iY_2$

such that the conclusions of LEMMA VIII are satisfied for Y_2 by the $(n-\rho)\times(n-\rho)$ unimodular matrix U_a. Then if $Y_2^0 \gg 0$, we see that the series

$$\sum_{U_2 \notin S} \theta_{m,T_{12}}{}^k(Z_1, Z_{12}U_2)^l \epsilon(klm(Z_2[U_2]-Z_2[U_a]))$$

converges uniformly for $Z \in \mathcal{U}(Y_2^0)$, $Z_2 \in D_{U_a}'$. Denote this series by $\boldsymbol{S}_{m,T_{12}}{}^{kla}$. Then choose Y_2^0 such that

$$|\boldsymbol{S}_{m,T_{12}}{}^{kla}(Z)| < \min(\tfrac{1}{2}\eta(C)\kappa^C, \tfrac{1}{2}\eta(C))$$

for fixed large m and all k, l, a, and T_{12} an even rational multiple of mE, provided $Z \in \mathcal{U}(Y_2^0)$ and $Z_2 \in D_{U_a}'$. Since $\Phi_{m,T_{12}}{}^{kl}$ are invariant under $G_0'N_\rho$ and approach 0 as $Z \to V_{n-1}^*$, they induce holomorphic functions (4) $\Omega_{T_{12}kl}$ on a neighborhood $\mathfrak{U}$ of x, and it is clear that $V_{n-1}^* \cap \mathfrak{U} \subset V(\{\Omega_{T_{12}kl}\})$, where we may assume $\phi_n^{-1}(V_n \cap \mathfrak{U}) \cap F_n \subset \mathcal{U}(Y_2^0)$. We now show that $V(\{\Omega_{T_{12}kl}\}) \cap V_n \cap \mathfrak{U}$ is empty. For this, it suffices to show that $V(\{\Phi_{m,T_{12}}{}^{kl}\}) \cap \mathcal{U}(Y_2^0)$ is empty for some given fixed m. Let $Z \in \mathcal{U}(Y_2^0)$, assume $Z_2 \in D_{U_a}'$, and let k, T_{12} be such that $|\theta_{m,T_{12}}{}^k(Z_1, Z_{12}U_a)| \geqq \kappa$. Then

$$|\boldsymbol{S}_{m,T_{12}}{}^{kl}(Z)/\theta_{m,T_{12}}{}^k(Z_1, Z_{12}U_a)^l| \leqq \min(\tfrac{1}{2}\eta(C)\kappa^{C-l}, \tfrac{1}{2}\eta(C)\kappa^{-l}) \leqq \tfrac{1}{2}\eta(C).$$

Therefore, by LEMMA VI, $V(\{\Phi_{m,T_{12}}{}^{kl}\}) \cap \mathcal{U}(Y_2^0)$ is empty, and therefore $V(\{\Omega_{T_{12}kl}\}) \cap \mathfrak{U} = V_{n-1}^* \cap \mathfrak{U}$. Thus, V_{n-1}^* has a local basis at x, and we have therefore established

THEOREM 3. *V_{n-1}^* has a local basis at each $x \in V_n^*$.*

Combining this with Theorem 2 and the fact that V_0^* and V_1^* are general analytic spaces we obtain by an obvious induction

THEOREM 4. *V_n^* is a general analytic space.*

We shall now obtain

THEOREM 5. *The general analytic space V_n^* is isomorphic, analytically, to a (analytically) normal projective variety.*

Proof. Let m_n be as in LEMMA I, let $p > 0$ be such that $m_n \mid p$, and let $\varphi_1, \cdots, \varphi_{s(p)}$ be a basis of the automorphic forms of weight p on V_n^*. We define a mapping $\varphi^p: V_n^* \to CP^{s(p)}$, where CP^s is the s-dimensional complex projective space, by $\varphi^p(x) = (\varphi_1(x), \cdots, \varphi_{s(p)}(x))$, which is well defined since $\varphi_1, \cdots, \varphi_{s(p)}$ are simply cross-sections of the analytic sheaf of germs of automorphic forms of weight p on V_n^*, and by LEMMA I $\varphi_1, \cdots, \varphi_{s(p)}$ have no common zeros on V_n^*. Let $\theta_p: V_n^* \times V_n^* \to CP^{s(p)} \times CP^{s(p)}$ be defined by

$\theta_p = \varphi^p \times \varphi^p$. Let Δ_p be the diagonal of $CP^{s(p)} \times CP^{s(p)}$ and let $D_p = \theta_p^{-1}(\Delta_p)$. D_p is a subvariety of $V_n^* \times V_n^*$. If $p_1, p_2, \cdots$ is a strictly increasing sequence of positive integers such that $m_n \mid p_1 \mid p_2 \mid \cdots$, it is clear that $D_{p_1} \supseteq D_{p_2} \supseteq \cdots$, so that for sufficiently large $p_k = N$, we have $D_{p_k} = D_{p_{k+1}} = \cdots$. Let $\mathfrak{D}$ be the diagonal of $V_n^* \times V_n^*$. It is evident by Lemma II that $D_N \cap (V_n \times V_n) = \mathfrak{D} \cap (V_n \times V_n)$. Hence if $x \in V_n^*$, $(\varphi^N)^{-1}\varphi^N(x) \cap V_n$ consists of at most one point. If $n = 1$, it is obvious that $(\varphi^N)^{-1}\varphi^N(x) \cap V_{n-1}^*$ is also discrete. If we assume, by induction, that $(\varphi^N \mid V_{n-1}^*)^{-1}(y)$ is discrete for each $y \in CP^{s(N)}$, it follows that $(\varphi^N)^{-1}(y)$ is discrete (i.e., 0-dimensional or empty) for all $y \in CP^{s(N)}$. Therefore, by a well-established property of analytic mappings,(1) we see that if $x \in V_n^*$ and if $\mathfrak{U}$ is a small neighborhood of x, then $\varphi^N(\mathfrak{U})$ defines an irreducible(4) germ of a variety at $\varphi^N(x)$, and hence $\varphi^N(V_n^*) = \mathfrak{V}$ is a complex analytic variety in $CP^{s(N)}$. Moreover, φ^N is one-to-one on an everywhere dense set of regular points, namely, the regular points of V_n. Let $\mathfrak{V}^\#$ be the (canonical) normal model of $\mathfrak{V}$, $\mathfrak{V}^\# \subset CP^r$. According to Zariski [17], algebraic normality implies analytic normality. Then to each pair consisting of a point y of $\mathfrak{V}$ and an irreducible branch $\mathfrak{V}_y$ of $\mathfrak{V}$ at y, there corresponds precisely one point of $\mathfrak{V}^\#$. So, just as in the proof of Theorem 1, we see that φ^N can be naturally lifted to an analytic isomorphism $\varphi^\#$ of V_n^* onto $\mathfrak{V}^\#$ such that we have the following commutative diagram:

$$\begin{tikzcd}
V_n^* \arrow[r, "\varphi^\#"] \arrow[dr, "\varphi"'] & \mathfrak{V}^\# \arrow[d, "\pi"] \\
& \mathfrak{V},
\end{tikzcd}$$

where $\varphi = \varphi^N$, π being the natural map. This completes the proof.

Now let f be meromorphic on H_n, let f be invariant under M_n, and let $n \geqq 2$. Let $x \in H_n$ and let M_{nx} be the finite subgroup of M_n leaving x fixed. Then in a small neighborhood $\mathfrak{U}$ of x, $f = h_1/h_2$, where h_1 and h_2 are holomorphic in $\mathfrak{U}$. h_1 and h_2 may not be invariant under M_{nx}, but in this case, we let h_2^* be the product of the translates of h_2 under all elements of M_{nx} *except* the identity; then if we put $g_1 = h_1 h_2^*$, $g_2 = h_2 h_2^*$, g_1 and g_2 are invariant under M_{nx}, though not relatively prime at x, and $f = g_1/g_2$ in a small neighborhood of x. Thus f naturally induces a meromorphic function f^* on $V_n \subset V_n^*$. Since $n \geqq 2$, $\dim V_n^* - \dim V_{n-1}^* = n > 1$. Therefore, by an easy generalization(5) of Levi's theorem on removable singularities of meromorphic functions [5], f^* is meromorphic on all of V_n^* and hence on $\mathfrak{V}^{\#}$. Since the correspondence π is birational, this means [1] that f^* is a rational function of the coordinates in $\mathfrak{V}$. From this, it follows that f is a quotient of homogeneous polynomials in $\varphi_1, \cdots, \varphi_{s(N)}$. We have therefore,

---

(5) Levi's theorem on removable singularities of meromorphic functions, as proved

THEOREM 5. *If f is a meromorphic function in H_n invariant under M_n, f is the quotient of two automorphic forms of like weight (though not, in general, everywhere relatively prime), provided $n \geqq 2$.*

It would be of interest to learn something of the Betti numbers, etc. of the space V_n^*, but nothing of this nature is known to the author. It would also be of interest to know the relationship between V_2^* and $\bar{V}_2$ (see [12]). It seems quite clear that V_2^* and $\bar{V}_2$ are birationally equivalent to each other and, by a result of Lapin [7], and others to CP^3. It is possible that $\bar{V}_2$ is obtained from V_2^* by a monoidal transformation along the irreducible subvariety V_1^*, but the author has no proof.

It will be shown in a later paper that if $M^{\#}$ is any subgroup of M_n of finite index (e.g., one of its congruence subgroups), Satake's methods yield a compactification $V^{\#}$ of the quotient space $H_n/M^{\#}$ such that there is a natural analytic map $\nu: V^{\#} \to V_n^*$ having the following properties:

(1) ν is a proper map and if $x \in V_n^*$, $\nu^{-1}(x)$ is a finite set.

(2) There is a subvariety A of V_n^* of codimension $\geqq 1$ such that ν is a *locally* topological map of $V^{\#} - \nu^{-1}(A)$ onto $V_n^* - A$.

(3) If $x \in A$ and $x' \in \nu^{-1}(x)$, x' has a basis of neighborhoods $\{\mathfrak{U}_\alpha\}$ such that $\mathfrak{U}_\alpha \cap (V^{\#} - \nu^{-1}(A))$ is non-empty and connected.

Then combining this with the results we have already obtained, or, alternatively, using THEOREM 3 of this paper in conjunction with Theorem 3 of [4] and the remark following Theorem 1 of [3] we shall see that $V^{\#}$ is (analytically isomorphic to) a normal projective variety. We shall also obtain the analog of Theorem 5.

THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
THE UNIVERSITY OF CHICAGO.

---

in [5], applies only to meromorphic functions in an open domain of C^n. However, it is not hard to prove that if f is a meromorphic function on a normal general analytic space V of pure dimension n except possibly on an imbedded subvariety of (complex) dimension $\leqq n - 2$, then f is meromorphic on all of V. We omit the proof here.

REFERENCES.

[1] W. L. Chow, "On compact complex analytic varieties," *American Journal of Mathematics*, vol. 71 (1949), pp. 893-914.

[2] F. Conforto, *Abelsche Funktionen und Algebraische Geometrie*, Springer, Berlin, 1956.

[3] H. Grauert and R. Remmert, "Espaces analytiquement complets," *Comptes Rendus de l'Academie des Sciences*, vol. 245 (1957), pp. 882-885.

[4] ———, "Sur les revêtements analytiques des variétés analytiques," *Comptes Rendus de l'Academie des Sciences*, vol. 245 (1957), pp. 918-921.

[5] H. Kneser, "Ein Satz über die Meromorphiebereiche analytischer Funktionen von mehrerer Veränderlichen," *Mathematische Annalen*, vol. 106 (1932).

[6] M. Koecher, "Zur Theorie der Modulformen n-ten Grades I," *Mathematische Zeitschrift*, vol. 59 (1954), pp. 399-416.

[7] I. Lapin, "On the Theory of Siegel's Modular Functions of Degree 2," (in Russian), *Izvestiya Akademii Nauk*, vol. 20 (1956).

[8] H. Maass, "Über die Darstellung der Modulformen n-ten Grades durch Poincaréschen Reihen," *Mathematische Annalen*, vol. 123 (1951), pp. 125-51.

[9] H. Minkowski, *Gesammelte Abhandlungen*, B. G. Teubner, Berlin-Leipzig, 1911.

[10] K. Oka, "Sur les Fonctions Analytiques de Plusieurs Variables VIII—Lemme Fondamental (Suite)," *Journal of the Mathematical Society of Japan*, vol. 3, No. 2 (1951), pp. 259-278.

[11] R. Remmert and K. Stein, "Über die wesentliche Singularitäten analytischer Mengen," *Mathematische Annalen*, vol. 126 (1953), pp. 263-306.

[12] I. Satake, "On Siegel's Modular Functions," *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo-Nikko, 1955.

[13] ———, "On the Compactification of the Siegel Space," *Journal of the Indian Mathematical Society*, vol. 20 (1956), pp. 259-281.

[14] Séminaire de H. Cartan, 1951-1952 (hectographed notes).

[15] Séminaire E. N. S., 1953-1954 (hectographed notes).

[16] C. L. Siegel, "Einführung in die Theorie der Modulfunktionen n-ten Grades," *Mathematische Annalen*, vol. 116 (1938-1939), pp. 617-657.

[17] O. Zariski, "Sur la normalité des variétés normales," *Annales de l'Institut Fourier* (Université de Grenoble), vol. 2 (1950), pp. 161-164.

EIGENFUNCTION EXPANSIONS FOR NON-SYMMETRIC PARTIAL DIFFERENTIAL OPERATORS, I.*

By Felix E. Browder.

Introduction. Let L and B be two differential operators defined on a domain G of Euclidean n-space E^n $(n \geqq 1)$. By an eigenfunction expansion for L with respect to B on G is meant, roughly speaking, a sequence of measures $\{m_j\}$ on the complex plane and a sequence of functions $\{u_j(x,\zeta)\}$ defined for x in G and ζ complex, such that:

(a) $(L-\zeta B)u_j(x,\zeta)=0$,

(b) For a suitably smooth function v in a restricted class, $U_j(v)(\zeta) = \int_G (Bv)(x)\overline{u_j(x,\zeta)}\,dx$ is defined except on a set of m_j-measure zero and lies in $L^2(m_j)$ while $(Bv,v)=\sum_j \int |U_j(v)(\zeta)|^2\,dm_j(\zeta)$,

(c) $v(x)=\sum_j \int U_j(v)(\zeta)u_j(x,\zeta)\,dm_j(\zeta)$.

The general theory of eignefunction expansions for singular self-adjoint ordinary differential operators was initiated by Weyl in 1910 with his treatment of the second-order case, and has been intensively developed since that time.[1] Two simplifying circumstances are present in the case of ordinary differential operators as contrasted with partial differential operators proper $(n \geqq 2)$. The first and most important is that the family of solutions of a linear ordinary differential equation is of finite linear dimension, so that many questions about it can be reduced to problems in finite-dimensional linear algebra. Second, from the point of view of the theory of partial differential operators, an ordinary differential equation is both elliptic, so that all its solutions are smooth functions, and hyperbolic, so that the Cauchy problem has a stable solution. It is not surprising, therefore, that it has been possible to obtain eigenfunction expansions for general classes of

---

* Received October 31, 1957; revised January 15, 1958.

[1] An inclusive account of the theory for ordinary differential operators is given by Coddington and Levinson [12].

ordinary differential operators by the methods of classical analysis, while in the case of partial differential operators proper, it has been necessary to have recourse to the tools furnished by functional analysis.

Except for the work of Carleman in 1934 on the Schroedinger equation [10], the development of the theory of eigenfunction expansions for partial differential operators has taken place only in recent years. In 1953, using an argument already set forth in general terms by Mautner [22] and based upon the Von Neumann-Stone spectral theory for unbounded self-adjoint operators, Gårding ([14], [15]) and the writer [7] independently proved the existence of an eigenfunction expansion corresponding to each self-adjoint realization of a formally self-adjoint elliptic partial differential operator.[2] For differential operators with constant coefficients, an extension to hypoelliptic operators was given in 1955 by Hormander [20]. In 1955, Gelfand and Kostyucenko announced in [17] the existence of an eigenfunction expansion for each self-adjoint realization of a formally self-adjoint partial differential operator without any requirement of ellipticity. Basing their proof upon a Banach space differentiation theorem due to Gelfand [16], they obtained eigenfunctions which were in the general case distributions of some prescribed order. Using the same differentiation theorem in Hilbert space (where it was first proved by G. Birkhoff [4]), the present writer in [8] extended their result to obtain eigenfunction expansions for formally self-adjoint partial differential operators of arbitrary type without any assumption on the existence of self-adjoint realizations.[3]

In the present paper, we establish more generally an eigenfunction expansion theorem for any subnormal realization A of a partial differential operator L in $L^2(G)$. The class of (possibly unbounded) subnormal operators which includes all symmetric operators is defined by one of the two equivalent conditions: A is subnormal if it can be extended to a normal operator in a larger Hilbert space, or if it can be written in the form $A = \int \zeta \, dF(\zeta)$, where F is a positive operator-valued measure on the Borel sets of the complex plane C^1 with $\| Au \|^2 = \int | \zeta |^2 \, d[F_\zeta u, u]$. The proof for subnormal operators is based upon the Birkhoff-Gelfand differentiation theorem, and the eigenfunctions obtained are distribution solutions of the equation $(L - \zeta)u$

---

[2] See also the paper of Povsner [26] on the Schroedinger equation where related methods are applied. Another proof for self-adjoint realizations of elliptic operators was later given by Bade and Schwartz [2].

[3] The proof of the result announced in [17] was published by Gelfand and Silov [18]. Another proof has been given by Berezanski [3]. At the same time as the writer's paper [8], results in the symmetric case for ordinary differential operators were obtained by Coddington [11].

$=0$. In particular, by applying results on the smoothness of solutions of hypoelliptic equations, one obtains for such operators eigenfunction expansions in the classical sense.

If B is a positive partial differential operator on G, we also obtain a proof of an expansion theorem in solutions of $(L.-\bar{\zeta}B)u=0$ under the assumption that L has a subnormal realization in a Hilbert space H_B defined by the operator B. In this case (as in a corresponding argument indicated for self-adjoint operators on E^n by Gelfand and Kostyucenko [17], [18]), the eigenfunctions obtained are no longer distributions in general, but, rather, linear functionals of a more general type, and it becomes impossible to rely upon results on the smoothness of distribution solutions of hypoelliptic equations. We shall treat this difficulty in the following paper of the present series.

Section 1 discusses subnormal operators, their generalized spectral resolutions, and various operator-theoretical results applied in the subsequent discussion. In Section 2, the Hilbert spaces which we shall use are defined and their properties established. In Section 3, the proof is given of the existence of an eigenfunction expansion corresponding to each generalized spectral resolution of a subnormal operator. Section 4 treats of hypoelliptic operators.

Section 1. Let H be a Hilbert space with inner product $[u,v]$, T a (possibly unbounded) linear operator with domain D_T dense in H and range R_T in H, T^* the adjoint of T. Since we shall assume that T has a closure in H, T^* is a closed, densely defined linear operator in H. T is said to be normal if $TT^*=T^*T$, with the usual convention for the multiplication of unbounded operators. By the spectral theorem, every normal operator T in H has a resolution of the identity $\{E_\zeta\}$, i.e., a function E from the σ-algebra Ω of Borel sets of C^1, the complex plane, to the projections of H such that: (1) $E(C^1)=I$, the identity operator; for each u in H, $[E(S)u,u]$ is a positive measure on Ω; (2) $u\in D_T$ if and only if $\int |\zeta|^2\, d[E_\zeta u,u]<\infty$; If $u\in D_T, v\in H$, $[Tu,v]=\int \zeta\, d[E_\zeta u,v]$; (3) $E(S_1\cap S_2)=E(S_1)E(S_2)$ for S_1, S_2 in Ω.

Definition 1. T is subnormal if there exists a Hilbert space H_1 containing H as a closed subspace and a normal operator T_1 in H_1 such that $T\subseteq T_1$.

For bounded operators, Definition 1 coincides with that given by Halmos in [19]. Halmos has given a characterization of bounded subnormal operators which in the simplified expression given to it by Bram [5] is the following: the bounded operator T is subnormal if for every finite family of elements $u_1, \cdots, u_r$ of H,

$$\sum_{j,k=1}^{r} [T^j u_k, T^k u_j] \geqq 0. \tag{1}$$

In the more general case of unbounded operators, every operator T admitting a normal extension in H itself is trivially subnormal. By a theorem of Neumark ([1]), every symmetric operator has a self-adjoint extension in a larger Hilbert space and therefore is subnormal.

Remark. We shall call T formally normal if $D_T \subset D_{T^*}$ and $\| Tu \| = \| T^* u \|$ for u in D_T. One might conjecture that every formally normal operator T is subnormal. The truth or falsity of this conjecture does not seem easy to establish, especially in view of the meagreness of studies as to conditions for the extendability of a formally normal operator to a normal operator in H itself. (See [21], [24], [25]). If it were true that every formally normal operator were subnormal, then it would follow from the argument employed in the case of bounded operators that if $R_T \subset D_T$ and (1) holds for every sequence chosen from D_T, then the unbounded operator T would be subnormal.

Definition 2. Let T be a subnormal operator in H, T_1 a normal extension of T to a Hilbert space H_1 containing H as a closed subspace, P the projection of H_1 on H, $\{E_\zeta\}$ the resolution of the identity of T_1 in H_1. Then the generalized spectral resolution of T corresponding to T_1 is the function F from the σ-algebra Ω of Borel subsets of C^1 to $L(H)$ (the set of bounded linear operators on H) defined by $F(S) = PE(S)$.

We note some of the properties of such a generalized spectral resolution:

(a) $F(C^1) = I$; for $u \in H$, $[F(S)u, u]$ is a positive measure on Ω.

(b) If $u \in D_T$, $\int_{C^1} |\zeta|^2 \, d[F_\zeta u, u] = \| Tu \|^2$.

(c) For $u \in D_T$, $v \in H$, $[Tu, v] = \int_{C^1} \zeta \, d[F_\zeta u, v]$.

LEMMA 1. *Let T be a linear operator in H, F a function from Ω to $L(H)$ for which* (a), (b), *and* (c) *are true. Then T is subnormal and $\{F_\zeta\}$ is the generalized spectral resolution of T corresponding to some normal extension T_1 of T.*

Proof. It follows from (a) that for each S in Ω, $F(S)$ is self-adjoint. By a theorem of Neumark (cf. [23], p. 28), there exists a Hilbert space H_1 containing H as a closed subspace and a resolution of the identity $\{E_\zeta\}$ in H_1 such that, if P is the projection of H_1 on H, then $PE(S) = F(S)$ for all S in Ω. Corersponding to this resolution of the identity, there is a normal operator T_1 in H_1 with $D_{T_1} = \{w \mid \int_{C^1} |\zeta|^2 d[E_\zeta w, w] < \infty\}$ while for $w \in D_{T_1}$, $v \in H_1$

$$[T_1 w, v] = \int_{C^1} \zeta \, d[E_\zeta w, v].$$

For $u \in H$, $[E_\zeta u, u] = [F_\zeta u, u]$, and (b) implies that D_T is contained in D_{T_1}. For $u \in D_T$, $v \in H$ the chain of equalities

$$[E_\zeta u, v] = [Pu, E_\zeta v] = [u, F_\zeta v] = [F_\zeta u, v]$$

implies that $[Tu, v] = \int_{C^1} \zeta \, d[F_\zeta u, v] = \int_{C^1} \zeta \, d[E_\zeta u, v] = [T_1 u, v]$. Thus $T \subseteq PT$, while (b) implies $T \subseteq T_1$.

Let T be a subnormal operator in H, $\{F_\zeta\}$ a generalized spectral resolution corresponding to T. Let T_1 be a normal extension of T in a Hilbert space H_1 with projection P on its closed subspace H, $\{E_\zeta\}$ the spectral resolution of T_1 with the property that $PE(S) = F(S)$. If g is an arbitrary element of H_1, we define $H_1(g)$, the cyclic subspace generated by g with respect to $\{E_\zeta\}$, to be the subspace of H_1 spanned by $E(S)g$ with S ranging over the Borel sets of C^1. It follows by a familiar argument that if h lies in the orthogonal completment of $H_1(g)$, so does $H_1(h)$, and we may select an indexed set $\{g_\beta : \beta \in Q\}$ in $H_1 = \sum_{\beta \in Q} \oplus H_1(g_\beta)$.

LEMMA 2. *If H is separable, H_1 and T_1 may be chosen so that Q is countable.*

Proof. Let Q' be any subset of Q, $H' = \sum_{\beta \in Q'} \oplus H_1(g_\beta)$, T' the restriction of T_1 to $H' \cap D(T_1)$. Then the range of T' is contained in H', T' is a normal operator with dense domain in H', and if $\{E'_\zeta\}$ is its spectral resolution, E'_ζ is the restriction of E_ζ to H'.

Let $\{h_k\}$ be a dense sequence in the separable Hilbert space H. For each k, h_k has a non-zero projection on $H_1(g_\beta)$ only for β in a countable set Q_k. If we set $Q' = \bigcup_k Q_k$, Q' is countable, and $H \subset \sum_{\beta \in Q'} \oplus H_1(g_\beta) = H'$. Further, for $\beta \in Q'$, the cyclic subspace generated by g_β with respect to $\{E'_\zeta\}$ is equal to $H_1(g_\beta)$ while, if P' is the projection of H' on H, $F(S) = P'E'(S)$. H' and T' are the sought extensions. If $H_1 = H$, then $H' = H$.

To conclude the present section, we establish the following lemma which is applied in the proof of our main theorem.

LEMMA 3. *Let m be a positive finite measure on the σ-algebra Ω of Borel set of C^1, h a vector-valued measure on Ω with values in a Hilbert space H_0. Suppose that h is weakly absolutely continuous with respect to m and that there exists a constant K such that for any finite pairwise disjoint family S_k of sets of Ω, $\sum_k \| h(S_k) \| \leqq K$. Then there exists an m-integrable function u from C^1 to H_0 such that, for $S \in \Omega$, $\psi \in H_0$,*

$$[h(S), \psi] = \int_S [u(\zeta), \psi] dm(\zeta).$$

Proof. To reduce the lemma to the theorem of Birkhoff [4] and Gelfand ([16], pp. 260-266), of which it is a variant, we apply the method of Riesz-Sz. Nagy ([28], Sec. 60, pp. 130-131) to obtain a mapping f of a Borel set Z of the unit interval J onto a Borel set C' of C^1 such that, if m_L denotes Lebesgue linear measure, $m_L(Z) = 1$, $m(C') = m(C^1)$, while $m_L(f^{-1}(S)) = m(S)$ for each Borel subset S of C'. The mapping f, as well as f^{-1}, carries Borel sets into Borel sets, and f is one-to-one on the complement of a countable, pairwise disjoint family of intervals $\{Z_j\}$, each of which is mapped by f on a point x_j of C^1 having a non-zero measure with respect to m.

Let $Z_1 = Z - \bigcup_j Z_j$, S a Borel set of J. Let h_1 be defined by

$$h_1(S) = h(f(S \cap Z_1)) + \sum_j h(x_j) m(S \cap Z_j).$$

It is easy to verify that h_1 is a vector-valued measure on the Borel sets of J which is weakly absolutely continuous with respect to m_L and satisfies the bounded-variation condition of the hypothesis for h. By the theorem of Birkhoff-Gelfand, h_1 has a strong derivative a.e. on J, and if we set $dh_1/dt = u(t)$, u is strongly m_L-integrable and $h_1(S) = \int_S u(t) dm_L(t)$. On each Z_j, $u(t)$ is the constant $h(x_j)$. Thus, if $f(t) = x$, $u(t)$ is uniquely defined by x on C'. The function $u(x)$ thus defined (and set equal to zero outside of C') is m-measurable, and by the transformation formulae for integrals,

$$[h(S), \psi] = \int_S [u(\zeta), \psi] dm(\zeta)$$

for each $\psi \in H_0$, S in Ω.

Section 2. Let G be an open set in the n-dimensional Euclidean space

E^n with points $x = (x_1, \cdots, x_n)$, $C_c^\infty(G)$ the family of complex-valued infinitely differentiable functions with compact support in G, $L^2(G)$ the Hilbert space of equivalence classes of complex-valued square-summable functions with inner product $(u, v) = \int u(x)\bar{v}(x)\,dx$ ($\bar{v}$ the complex conjugate of v, integration with respect to Lebesgue n-measure). If α is a multi-index $(\alpha_1, \cdots, \alpha_r)$ with $1 \leqq \alpha_j \leqq n$, we shall let $|\alpha| = r$ while $D^\alpha = \partial^r / \partial x_{\alpha_1} \cdots \partial x_{\alpha_r}$. (For the empty set of indices ϕ, we let $D^\phi = I$.).

Let $C^j(G) = \{f \mid f$ is defined in G, $D^\alpha f$ exists and is continuous in G for $|\alpha| \leqq j\}$.

Let B be a linear operator with $C_c^\infty(G)$ as its domain and its range contained in the linear space of locally square-summable functions on G. We shall assume that there exist $p \in C^0(G)$, $N \in C^r(G)$ for some $r \geqq 0$ with $p(x) > 0$ in G, $N(x) > 0$ for x in G, such that:

$$\text{(2)} \qquad \text{For } \phi, \psi \in C_c^\infty(G),\ (B\phi, \psi) = (\phi, B\psi),\ (B\phi, \phi) \geqq (p\phi, \phi);$$

$$\text{(3)} \qquad (B\phi, \phi) \leqq \sum_{|\alpha| \leqq r} (ND^\alpha\phi, D^\alpha\phi), \qquad \phi \in C_c^\infty(G);$$

$$\text{(4)} \qquad (p^{-1}B\phi, B\phi) < \infty \text{ for } \phi \in C_c^\infty(G).$$

(Note that if B is a differential operator, (4) is automatically satisfied.)

On $C_c^\infty(G)$, we define the B-inner product by,

$$\text{(5)} \qquad [\phi, \psi] = (B\phi, \psi);\ \phi, \psi \in C_c^\infty(G).$$

The family of functions $C_c^\infty(G)$ with its ordinary linear structure and the inner product $[\ ,\ ]$ is a pre-Hilbert space.

Definition 3. H is the Hilbert space which is the completion of $C_c^\infty(G)$ with respect to the norm $\| u \|_H = [u, u]^{\frac{1}{2}}$.

Let $L^2(p)$ be the Hilbert space of equivalence classes of locally square-summable functions u for which $(pu, u) < \infty$ with inner product (pu, v) and norm $(pu, u)^{\frac{1}{2}}$. By (2), every Cauchy sequence from $C_c^\infty(G)$ in H-norm is also a Cauchy sequence in $L^2(p)$. Thus, there exists a continuous mapping J of H into $L^2(p)$ which is the identity mapping on $C_c^\infty(G)$. We assert that J is one-to-one; for if $\{\phi_s\}$ is a sequence from $C_c^\infty(G)$, converging to h in H with $(p\phi_s, \phi_s) \to \infty$, and if $\psi \in C_c^\infty(G)$, we have $[h, \psi] = \lim\limits_{S} [\phi_s, \psi]$ $= \lim\limits_{S} (\phi_s, B\psi)$. Now $|(\phi_s, B\psi)|^2 \leqq (p\phi_s, \phi_s)(p^{-1}B\psi, B\psi) \to 0$ as $s \to 0$ by (4). But then $[h, \psi] = 0$ for all ψ in $C_c^\infty(G)$ and $h = 0$ since $C_c^\infty(G)$ is dense in H. Thus H may be identified with a linear subset of $L^2(p)$. If p_1 is any other positive continuous function on G with $p_1(x) \leqq p(x)$ for x in G, then obviously $L^2(p)$ is a linear subset of $L^2(p_1)$ and H may be identified with a subset of $L^2(p_1)$ and H may be identified with a subset of $L^2(p_1)$.

Given $N \in C^r(G)$, $N(x) > 0$ in G, $r \geqq 0$, we define the (N,r)-inner product on $C_c^\infty(G)$ by $[u,v]_{N,r} = \sum_{|\alpha| \leqq r} (ND^\alpha u, D^\alpha v)$. If the differential operator B_1 is defined by $B_1 u = \sum_{|\alpha| \leqq r} (-1)^{|\alpha|} D^\alpha (N(x) D^\alpha u)$, then $[u,v]_{N,r} = (B_1 u, v)$ for $u, v \in C_c^\infty(G)$, and B_1 satisfies the conditions (2), (3), and (4) on B with the pair of functions (p,N) replaced by (N,N). If we complete $C_c^\infty(G)$ with respect to this inner product to a Hilbert space $H_{N,r}$, there will be a continuous one-to-one mapping J_1 of $H_{N,r}$ into $L^2(p_1)$, where $p_1(x) = \min\{p(x), N(x)\}$, which is the identity mapping on $C_c^\infty(G)$. Furthermore, (3) implies that there exists a continuous mapping J_2 of $H_{N,r}$ into H which is the identity mapping on $C_c^\infty(G)$. Let J_3 be the imbedding mapping of H into $L^2(p_1)$. Then $J_1 = J_3 J_2$, and since J_1 and J_3 are one-to-one, J_2 must be one-to-one and $H_{N,r}$ may be identified with a linear subset of H.

As a special case of the spaces $H_{N,r}$, we may choose $N(x) \equiv 1$, and designate the corresponding Hilbert spaces and inner products by H_r and $[u,v]_r$. If G is bounded, $r_1 > r$, by a well-known lemma of Rellich (e.g., [6], p. 32), it follows that the imbedding map $J_{r_1 r}$ of H_{r_1} into H_r is compact. For bounded G, the inner product $[u,v]'_r = \sum_{|\alpha| = r} (D^\alpha u, D^\alpha v)$ yields a norm on H_r equivalent to the r-norm. We designate the Hilbert space with the inner product $[\ ,\ ]'_r$ on H_r by H'_r.

LEMMA 4. *Suppose $f \in C^0(G)$ with $f(x) > 0$ for x in G, $r \geqq 0$. Then there exists $g \in C(G)$ with $g(x) > 0$ in G, such that*

$$|D^\alpha g(x)| \leqq f(x)$$

for all x in G and all $|\alpha| \leqq r$.

The proof of Lemma 4 follows from a standard argument using an infinitely differentiable partition of unity corresponding to a suitably fine locally finite covering of G.

LEMMA 5. *Let G be a bounded open set in E^n, $r \geqq 0$, $r_1 = r + n + 1$. Then there exists a unique compact self-adjoint positive linear operator C_r on H'_{r_1}, such that*

$$[u,v]_r = [C_r u, v]'_{r_1}$$

for $u, v \in H'_{r_1}$. Further, if $\{\lambda_{k,r}\}$ is the sequence of eigenvalues of C_r in non-

increasing order corresponding to a complete orthonormal set in H'_{r_1}, *we have* $\sum_{k=1}^{\infty}\{\lambda_{k,r}\}^{\frac{1}{2}} < \infty$.

Proof. For fixed u in H'_{r_1}, $[u,v]'_r$ is a continuous conjugate-linear functional of v on H'_{r_1}. Hence, there exists a unique element w in H'_{r_1} such that $[u,v]'_r = [w,v]'_{r_1}$ for all v in H'_{r_1}. If we set $C_r u = w$, it follows that $\| C_r u \|'_{r_1} \leqq c_r \| u \|'_r$, and by the lemma of Rellich mentioned above, C_r is a compact linear operator on H'_{r_1}. Further, C_r is self-adjoint and positive on H'_{r_1} since $[C_r u, u]'_{r_1} = [u,u]'_r > 0$ for $u \neq 0$ in H'_{r_1}.

If $r = 0$, it follows from results on the asymptotic distribution of eigenvalues for the Dirichlet problem for a polyharmonic equation [13] that $\lambda_{k,0} \sim C(n,G)k^{-2-2/n}$, and therefore $\sum_{k=1}^{\infty}\lambda_{k,0}^{\frac{1}{2}} < \infty$.

For $r > 0$, we define $W = \sum_{|\alpha|=r} \oplus H^{\alpha}_{n+1}$, where, for each α, H^{α}_{n+1} is a copy of H'_{n+1}. If $v = \{v_\alpha\}$ is an element of W, let $\| v \|_0{}^2 = \sum_{|\alpha|=r} \| v_\alpha \|_0{}^2$. We define a mapping T of H'_{r_1} into W by setting $Tu = \{u_\alpha\}$, where the α-th coordinate $u_\alpha = D^\alpha u$. Then T is a one-to-one mapping of H'_{r_1} into W, and there exists a constant $c_1 > 0$ such that $\| Tu \|_W{}^2 \leqq c_1[\| u \|'_{r_1}]^2$. Moreover, $\| Tu \|_0{}^2 = [\| u \|'_r]^2$. By the minimax principle for eigenvalues of compact self-adjoint operators on a Hilbert space ([27], p. 235),

$$\lambda_{k,r} = \max_{S_k \subset H'_{r_1}} \{\min\{[\| u \|'_r]^2/[\| u \|'_{r_1}]^2 ; u \in S_k\}\},$$

where the maximum is taken over all subspaces S_k of linear dimension k in H'_{r_1}. For each u in H'_{r_1}, $c_1[\| u \|'_r]^2/[\| u \|'_{r_1}]^2 \leqq \| Tu \|_0{}^2/\| Tu \|_W{}^2$. Since T is one-to-one, it follows that $c_1\lambda_{k,r} \leqq \xi_{k,r}$, where

$$\xi_{k,r} = \max_{S'_k \subset W} \{\min\{\| v \|_0{}^2/\| v \|_W{}^2 ; v \in S'_k\}\},$$

where the S'_k range over the k-dimensional subspaces of W.

If $v = \{v_\alpha\}$, $\| v \|_0{}^2 = \sum_{|\alpha|=r} [C_0 v_\alpha, v_\alpha]'_{n+1}$. Thus $\{\xi_{k,r}\}$ is the sequence of eigenvalues of the operator $C'v = \{C_0 v_\alpha\}$. The only admissible values for the $\xi_{k,r}$ are the values taken on by various $\lambda_{j,0}$ and if $\xi_{k,r} = \lambda_{j,0}$, the multiplicity of $\xi_{k,r}$ as an eigenvalue of C' is $2^r(r!)^{-1}$ times the corresponding multiplicity for $\lambda_{j,0}$. Thus $\xi_{2^r(r!)^{-1}k,r} = \lambda_{k,0}$, and as a consequence,

$$\xi_{k,r} \sim c'(n,r,G)k^{-2-2/n}.$$

Finally, $\sum_{k=1}^{\infty}\lambda_{k,r}^{\frac{1}{2}} \leqq c_1^{-\frac{1}{2}}\sum_{k=1}^{\infty}\xi_{k,r}^{\frac{1}{2}} < \infty$.

THEOREM 1. *Let* G *be an open set of* E^n, $r \geqq 0$ $r_1 = r + n + 1$, $N(x) > 0$ *with* $N \in C^r(G)$. *Then there exist* $M \in C^\infty(G)$ *with* $M(x) \geqq N(x)$ *for* x *in* G *and a complete orthonormal sequence* $\{v_k\}$ *in* H_{M,r_1} *such that* $\sum_{k=1}^{\infty} \| u_k \|_{N,r} < \infty$.

Proof. We remark first that if the theorem is true for a given domain G, it is also true for any domain G_1 which is mapped by a C^∞-homeomorphism onto G. Since there exists a C^∞-homeomorphism of E^n onto its open unit ball, i. e., the set $|x| < 1$, we may assume without loss of generality that G is bounded.

Since G is assumed bounded, the lemma of Rellich cited above is valid for G. On the other hand, by Lemma 4, there exists $g \in C^\infty(G)$ with $g(x) > 0$ for all x in G, such that $|D^\alpha g(x)| \leqq N(x)^{-\frac{1}{2}}$ for $|\alpha| \leqq r$, $x \in G$. Let $\phi \in C_c^\infty(G)$. If we set $\psi = g^{-1}\phi$, we have,

$$\| \phi \|_{N,r}^2 = \sum_{|\alpha| \leqq r} (N^{\frac{1}{2}} D^\alpha(g\psi), N^{\frac{1}{2}} D^\alpha(g\psi)).$$

By the Leibniz formula for the differentiation of products,

$$D^\alpha(g\psi) = \sum_{\pi+\beta=\alpha} c_{\pi\beta} D^\pi(g) D^\beta(\psi),$$

with $c_{\pi\beta}$ positive constants. It follows that $|N^{\frac{1}{2}} D^\alpha(g\psi)| \leqq \sum_{\pi,\beta} c_{\pi\beta} |D^\beta \psi|$. Thus there exists $c > 0$ such that

$$\| \phi \|_{N,r}^2 \leqq c \| \psi \|_r^2. \tag{6}$$

In addition, we can obviously find a function M in $C^\infty(G)$ with $M(x) > 0$ for $x \in G$, such that

$$\| \psi \|_{r_1}^2 = \sum_{|\beta| \leqq r_1} (D^\beta(g^{-1}\phi), D^\beta(g^{-1}\phi)) \leqq \sum_{|\beta| \leqq r_1} (M D^\beta \phi, D^\beta \phi) = \| \phi \|_{M,r}^2 \tag{7}$$

for all $\phi \in C^\infty(G)$.

From (7), it follows that if a sequence $\{\phi_k\}$ from $C_c^\infty(G)$ is bounded in (M, r_1)-norm, the corresponding sequence $\{\psi_k\}$ with $\psi_k = g^{-1}\phi_k$, is bounded in r_1-norm. By the Rellich lemma, there exists a subsequence $\{\psi_{k_j}\}$ which is a Cauchy sequence in r-norm. By (6), the corresponding subsequence $\{\phi_{k_j}\}$ is a Cauchy sequence in (N, r)-norm. Thus $[u, v]_{N,r}$ is a completely continuous form on H_{M,r_1}, and there exists a compact linear self-adjoint operator C on H_{M,r_1} such that $[u, v]_{N,r} = [Cu, v]_{M,r_1}$ for all v in H_{M,r_1}.

We choose the sequence $\{v_k\}$ in H_{M,r_1} to be a complete orthonormal sequence of eigenfunctions of the compact positive operator C with a corresponding sequence of eigenvalues $\{\lambda_k\}$, which we may assume to be arranged in a non-increasing order. If $Cv_k = \lambda_k v_k$, we have

$$\| v_k \|_{N,r}^2 = [v_k, v_k]_{N,r} = [Cv_k, v_k]_{M,r_1} = \lambda_k.$$

To complete the proof of the theorem, we must show that $\sum_{k=1}^{\infty} \lambda_k^{\frac{1}{2}} < \infty$.

If we apply the minimax principle, as in the proof of Lemma 3, we see that the k-th eigenvalue will not decrease if we increase the norm $\| \phi \|_{N,r}^2$ to the larger norm $c \| \psi \|_r^2$, with $\psi = g^{-1}\phi$, or to the even larger norm $c_1\{\| \psi \|_r'\}^2$. Similarly, the k-th eigenvalue will not decrease if we replace the norm $\| \phi \|_{M,r}^2$ in the denominator of the quotient by the smaller norm $\{\| \psi \|'_{r_1}\}^2$. It follows directly that $\lambda_k \leqq c_1 \lambda_{k,r}$ where $\lambda_{k,r}$ is the k-th eigenvalue of the operator C_r defined in Lemma 5. Since by Lemma 5, $\sum_{k=1}^{\infty} \lambda_{k,r}^{\frac{1}{2}} < \infty$, the conclusion of the theorem follows.

By the argument of the paragraph preceding Lemma 4, there is a continuous injective linear mapping J_4 of H_{M,r_1} into H which is the identity on $C_c^{\infty}(G)$. Since H may be identified with its own conjugate space by the assignment $u \rightarrow [v, u]$, with the latter considered as an element of H^*, the adjoint mapping J_4^* may be considered as a continuous linear mapping of H into H^*_{M,r_1}. Since J_4 is one-to-one, the image of J_4^* is dense. Since the image of J_4 in H_{M,r_1} contains the dense subset $C_c^{\infty}(G)$ and is itself dense, it follows that J_4^* is one-to-one. Thus J_4^* identifies H with a dense subset of H^*_{M,r_1}. If we define a $(M, -r_1, B)$-norm on H by the prescription

$$\| u \|_{M,-r_1,B} = \sup \{ | [\psi, u] | \cdot (\| \psi \|_{M,r_1})^{-1} \mid \psi \in H_{M,r_1} \},$$

we see that $\| u \|_{M,-r_1,B} = \| J_4^* u \|_{H^*_{M,r_1}}$. It follows that the completion of H with respect to the $(M, -r_1, B)$-norm is a Hilbert space $H_{M,-r_1,B}$ which is isomorphic to H^*_{M,r_1}. If $B = p(x)I$, the space $H_{M,-r_1,p}$ for $p \in C_c^{\infty}(G)$ is composed of distributions of order r_1 at most.

Section 3.

Definition 4. Let A be a subnormal operator in H, $\{F_\zeta\}$ a generalized spectral resolution corresponding to A. By an eigenfunction expansion corresponding to $\{F_\zeta\}$, we shall mean a sequence of positive, finite measures $\{m_j\}$ defined on the Borel σ-algebra Ω of the complex plane C^1 and a sequence of functions $\{u_j\}$ from C^1 to $H_{M,-r_1,B}$ having the following properties:

(1) For $v \in H_{M,r_1}$, $c_j(\zeta) = [v, u_j(\zeta)]$ lies in $L^2(m_j)$ and we have $\| v \|_H^2 = \sum_{j=1}^{\infty} \{\| c_j \|_{L^2(m_j)}\}^2$. Thus the mapping U defined by $Uv = \{c_j\}$ is an

isometric mapping of the dense subset H_{M,r_1} of H into $\sum_j \oplus L^2(m_j)$ and can be extended by continuity to an isometric mapping of H into $\sum_j \oplus L^2(m_j)$.

(2) Let $\{c_j\} \in \sum_j \oplus L^2(m_j)$, S a Borel set in C^1. Then $c_j(\zeta)u_j(\zeta)$ is a strongly integrable function from C^1 to $H_{M,-r_1,B}$ with respect to the measure m_j. If $h_{j,S} = \int_S c_j(\zeta)u_j(\zeta)\,dm_j(\zeta)$, the element $h_{j,S}$ of $H_{M,-r_1,B}$ always lies in H, and the sum $\sum_j h_{j,S}$ converges strongly in H to an element h_S with

$$\| h_S \|_H{}^2 \leqq \sum_j \{\| c_j \|_{L^2(m_j)}\}^2.$$

(3) If $\{c_j\} = U(f)$ for $f \in H$, S a Borel set of C^1, then

$$F(S)f = \sum_j \int_S c_j(\zeta)u_j(\zeta)\,dm_j(\zeta).$$

For $S = C^1$ and such an element $\{c_j\}$, equality holds in the inequality of (2).

(4) If $v \in D_A \cap H_{M,r_1}$, $Av \in H_{M,r^1}$, then for every $\zeta \in C^1$,

$$[u_j(\zeta), Av] = \bar{\zeta}[u_j(\zeta), v].$$

Definition 5. The eigenfunction expansion of Definition 4 is said to be full if the mapping U described in (1) maps H onto $\sum_j \oplus L^2(m_j)$. Then, for $S = C^1$, equality holds in the inequality of (2).

The basic result of the present paper is the following:

THEOREM 2. *Let A be a subnormal operator defined in the space H, $\{F_\zeta\}$ a generalized resolution of the identity corresponding to A. Then there exists an eigenfunction expansion corresponding to $\{F_\zeta\}$ and this expansion is full if F_ζ is an ordinary spectral resolution.*

Proof. There exists a Hilbert space H_1 containing H as a closed subspace and a normal operator T_1 in H_1 such that $T \subseteq T_1$ and $F(S) = PE(S)$, where $\{E_\zeta\}$ is the spectral resolution of T_1, and P is the projection of H_1 on H. If $\{F_\zeta\}$ is an ordinary spectral resolution, we choose H_1 to be equal to H itself.

By Lemma 2, we may assume that there exists a sequence $\{g_j\}$ in H_1 such that $H_1 = \sum_j \oplus H_1(g_j)$. Let $m_j(S) = [E(S)g_j, g_j]$. If we denote $H_1(g_j)$ by H_j, the mapping V_j assigning to a function $c_j \in L^2(m_j)$ the element $h_j = \int_{C^1} c_j(\zeta)\,dE_\zeta g_j$ is a unitary mapping of $L^2(m_j)$ onto H_j. Let $f \in H_1$. Then $f = \sum_j h_j$ with $h_j = V_j c_j \in H_j$. If $f \in H$, $Pf = f$ implies that

$f = \sum_j f_j$ with $f_j = Ph_j = \int_{C^1} c_j(\zeta)dF_\zeta g_j$. Moreover, $F(S)f = PE(S)f = \sum_j f_{j,S}$, where $f_{j,S} = PE(S)h_j = \int_S c_j(\zeta)\,dF_\zeta g_j$. In particular, the mapping U defined by $U(f) = \{c_j\}$ is an isometric mapping of H into $\sum_j \oplus L^2(m_j)$.

If, conversely, we are given an element $\{c_j\}$ of $\sum_j \oplus L^2(m_j)$, S a Borel set of C^1, we define $h_{j,S} = \int_S c_j(\zeta)\,dF_\zeta g_j$, $h_S = \sum_j h_{j,S}$, the sum converging strongly in H. Since $h_{j,S} = P(\int_S c_j(\zeta)\,dE_\zeta g_j)$, it follows that

$$\| h_S \|^2 \leqq \sum_j \| c_j \|^2_{L^2(m_j)}.$$

We must show the existence of a strongly m_j-measurable function u_j from C^1 to $H_{M,-r_1,B}$ such that, for all ψ in H_{M,r_1} and all Borel sets S of C^1,

$$[h_{j,S}, \psi] = \int_S c_j(\zeta)\,[u_j(\zeta), \psi]\,dm_j(\zeta). \tag{6}$$

Since $[h_{j,S}, \psi] = \int_S c_j(\zeta)\,d[F_\zeta g_j, \psi]$, it suffices that

$$[F(S)g_j, \psi] = \int_S [u_j(\zeta), \psi]\,dm_j(\zeta) \tag{7}$$

for all $\psi \in H_{M,r^1}$.

We shall verify that the assumptions of Lemma 3 are satisfied if $H_0 = H_{M,-r_1,B}$, $m(s) = m_j(S)$, and $h(S) = F(S)g_j$. (In the following argument we drop the subscript j from m_j and g_j.)

For $v \in H$,

$$|[h(S), v]| = |[PE(S)g, v]| = |[E(S)g, v]| \leqq m(S)\| v \|_H.$$

Thus h is weakly absolutely continuous with respect to m.

Let $\{S_k\}$ be a finite, pairwise disjoint family of Borel sets of C^1, $\psi \in H_{M,r_1}$. Then,

$$\begin{aligned} \sum_k |[h(S_k), \psi]| &= \sum_k [E(S_k)g, E(S_k)\psi]| \\ &\leqq \{\sum_k \| E(S_k)g \|_H{}^2\}^{\frac{1}{2}} \| \psi \|_H \leqq \| g \|_H \cdot \| \psi \|_H. \end{aligned} \tag{8}$$

Let $\{\psi_k\}$ be a sequence of elements from H_{M,r_1} with $\| \psi_k \|_{H_{M,r_1}} = 1$. By Theorem 1, there exists a complete orthonormal sequence $\{v_j\}$ in H_{M,r_1} with $\sum_j \| v_j \|_{N,r} < \infty$. Since $\| v \|_H \leqq \| v \|_{N,r}$, it follows that $\sum_j \| v_j \|_H < \infty$. Let $\psi_k = \sum_j a_{kj} v_j$ be the Fourier expansion of ψ_k *with* respect to this sequence.

Since $\| \psi_k \|_{M,r_1}{}^2 = 1 = \sum_j | a_{kj} |^2$, we have $| a_{kj} | \leqq 1$.

We choose the ψ_k so that $[h(S_k), \psi_k] = \| h(S_k) \|_{M,-r_1,B}$. Let

$$K = \| g \|_H \cdot \sum_j \| v_j \|_H < \infty .$$

Then,

$$\sum_k \| h(S_k) \|_{M,-r_1,B} = \sum_k [h(S_k), \psi_k] \leqq \sum_{k,j} | a_{jk} | \cdot | [h(S_k), v_j] | \leqq K. \tag{9}$$

Thus the hypotheses of Lemma 3 are satisfied, and we obtain a function u_j from C^1 to $H_{M,-r_1,B}$ satisfying (7).

To complete the proof of Theorem 2, we must verify properties (1) and (4) of Definition 4. Let $\psi \in H_{M,r_1}$, $f \in H_1$; and let $c_j(\zeta)$, $c'_j(\zeta)$ be the functions in $L^2(m_j)$ corresponding to the projections of ψ and f in H_j. By the spectral theory, $[f, \psi] = \sum_j \int c'_j(\zeta) \overline{c_j(\zeta)} \, dm_j(\zeta)$. On the other hand,

$$\begin{aligned}[f, \psi] &= \sum_j \int c'_j(\zeta) \, d[E_\zeta g_j, \psi] \\ &= \sum_j \int c'_j(\zeta) \, d[F_\zeta g_j, \psi] = \sum_j \int c'_j(\zeta) \, [u_j(\zeta), \psi] \, dm_j(\zeta),\end{aligned}$$

by the preceding part of the proof. Since $c'_j(\zeta)$, for $f \in H_1$, fills out the whole of $\sum_j \oplus L^2(m_j)$, we must have $c_j(\zeta) = [\psi, u_j(\zeta)]$ almost everywhere in m_j, and property (1) of Definition 4 is satisfied.

Similarly,

$$[f, Av] = \sum_j \int c'_j(\zeta) \bar{\zeta} \overline{c_j(\zeta)} \, dm_j(\zeta) = \sum_j \int c'_j(\zeta) \, [u_k(\zeta), Av] \, dm_j(\zeta)$$

implies that $[u_j(\zeta), Av] = \bar{\zeta} [u_j(\zeta), v]$ almost everywhere in m_j. We may alter the functions $u_j(\zeta)$ for ζ on sets of m_j-measure zero without affecting the validity of the other properties of the eigenfunction expansion. Let G be the graph of A as a mapping from H_{M,r_1} to H_{M,r_1} with its domain restricted to $D(A) \cap H_{M,r_1} \cap A^{-1}(H_{M,r_1})$. G is a closed subspace of the separable Hilbert space $H_{M,r_1} \times H_{M,r_1}$ and is therefore separable. Let (v_r, Av_r) be a dense sequence in G. To each r there corresponds an m_j-null exceptional set Q_r such that for $\zeta \notin Q_r$, $[u_j(\zeta), Av_r] = \bar{\zeta} [u_j(\zeta), v_r]$. On the complement of $Q = \bigcup_r Q_r$, which is a null set in m_j, $[u_j(\zeta), v] = \bar{\zeta} [u_j(\zeta), v]$ for all v. On Q, we set $u_j(\zeta) = 0$ and after this change on a m_j-null set, the last equality holds for all ζ. Thus the proof of the theorem is complete.

Section 4. Let L be a linear differential operator with coefficients in C^∞, $L = \sum_{|\beta| \leqq} c_\beta(x) D^\beta$. The adjoint operator L^+ of L is defined by $L^+(u) = \sum_\beta (-1)^{|\beta|} D^\beta (\bar{c}_\beta(x) u)$. Let B be a positive operator for which conditions (2)-(5) of Section 2 are valid. If ϕ and $\psi \in C_c^\infty(G)$,

$$|(L^+\phi, \psi)| \leqq c(\phi)(p\psi, \psi)^{\frac{1}{2}} \leqq c'(\phi) \| \psi \|_H.$$

Thus, there exists a unique element $A\phi$ in H such that $[A\phi, \psi] = (L^+\phi, \psi)$ for all $\psi \in C_c^\infty(G)$. Since $(L^+\phi, \psi) = (\phi, L\psi)$, A is a closable operator with domain $C_c^\infty(G)$ dense in H. If A is subnormal, we may apply Theorem 2 and get an eigenfunction expansion for A which is essentially in terms of eigenfunctions of $B^{-1}L$. We shall leave the discussion of the character of the eigenfunctions for general B to another place, and restrict ourselves for the remainder of this paper to the case when $B = p(x)I$, with $p(x) \in C_c^\infty(G)$.

THEOREM 3. *Let $p \in C_c^\infty(G)$ with $p(x) > 0$ in G, $B = p(x)I$, L a partial differential operator with infinitely differentiable coefficients, A the corresponding operator in the Hilbert space H as defined above. If A is subnormal in H, then the $u_j(\zeta)$ of Theorem 2 are distribution solutions of $(L - \bar{\zeta}p)u = 0$; i.e., $(u_j(\zeta), (L^+ - \zeta p)\phi) = 0$ for all ϕ in $C_c^\infty(G)$.*

Proof. From Theorem 2, we have $[u_j(\zeta), A\phi] = \bar{\zeta}[u_j(\zeta), \phi]$. Since convergence in $H_{M,-r_1,B}$ for $B = p(x)I$ implies convergence in the distribution sense, we obtain by a simple continuity argument $(u_j(\zeta), L^+\phi) = \bar{\zeta}(u(\zeta), P\phi)$.

Definition 6. The differential operator L is said to be hypoelliptic if for each integer j, $-\infty < j < \infty$, and $M \in C_c^\infty(G)$ with $M(x) > 0$ for x in G, there exists $M'_j \in C_c^\infty(G)$ with $M'_j(x) > 0$, such that every distribution solution of the equation $Lu = f$ with $f \in H_{M,j}(G)$ lies in $H_{M'_j, j+1}(G)$ and such that $\| u \|_{M'_j, j+1} \leqq \| f \|_{M,j} + \| u \|_{M,j}$.

THEOREM 4. *Let L be a hypoelliptic differential operator, $B = p(x)I$, with L having a subnormal realization A in H. Then the eigenfunctions $u_j(\zeta)$ of Theorem 2 are functions in $C^\infty(G)$, the integrals of Theorem 2 converge in the pointwise sense for ψ with compact support in G, and $\int_S |u_j(\zeta)|^2 \, dm_j(\zeta) < K(S, x)$, where $K(S, x)$ is bounded for S any bounded Borel set in C^1 and x is a compact subset of G.*

Proof. Applying the inequality of Definiton 6 to the distribution solution $u_j(\zeta)$ of the equation $Lu = pu$, we obtain a sequence of functions M_j such that $\| u \|_{M_j, j+1} \leqq \| u \|_{M_{j-1}, j}$ and u lies in $H_{M_j, j}$ for arbitrarily large j. By a theorem of Sobolev (see, for instances, [29]), u lies in $C^\infty(G)$. The convergence and boundedness properties follow from the iteration of these inequalities.

We remark that a general class of differential operators with variable coefficients including both elliptic and parabolic operators are hypoelliptic in the sense of Definition 6 [9].

YALE UNIVERSITY.

REFERENCES.

[1] N. I. Achieser and I. M. Glasmann, *Theories der linearen Operatoren im Hilbert-raum*, Berlin, 1954, Anhang I.

[2] W. G. Bade and J. T. Schwartz, "On Mautner's eigenfunction expansions," *Proceedings of the National Academy of Sciences*, vol. 42 (1956), pp. 519-525.

[3] Yu. M. Berezanski, "On expansion in eigenfunctions of general self-adjoint differential operators," *Doklady Akademii Nauk SSSR* (N. S.), vol. 108 (1956), pp. 379-382.

[4] G. Birkhoff, "Integration of functions with values in a Banach space," *Transactions of the American Mathematical Society*, vol. 38 (1935), pp. 357-378.

[5] J. Bram, "Subnormal operators," *Duke Mathematical Journal*, vol. 22 (1955), pp. 75-94.

[6] F. E. Browder, "Strongly elliptic systems of differential equations," *Annals of Mathematics Studies*, No. 33, 1954, pp. 15-51.

[7] ———, "Eigenfunction expansions for singular elliptic operators, I and II," *Proceedings of the National Academy of Sciences*, vol. 40 (1954), pp. 454-463.

[8] ———, "Eigenfunction expansions for formally self-adjoint partial differential operators, I and II," *ibid.*, vol. 42 (1956), pp. 769-771, 870-872.

[9] ———, "Regularity theorems for solutions of partial differential equations with variable coefficients," *ibid.*, vol. 43 (1957), pp. 234-236.

[10] T. Carleman, "Sur la théorie mathématique de l'équation de Schroedinger," *Arkiv för Matematik Astronomie o. Fysik*, vol. 24 (1934), No. 11, pp. 1-7.

[11] E. Coddington, "On maximal symmetric ordinary differential operators," *Mathematica Scandinavica*, vol. 4 (1956), pp. 22-28.

[12] ——— and N. Levinson, *Theory of Ordinary Differential Equations*, New York, 1954.

[13] L. Gårding, "The asymptotic distribution of the eigenvalues and eigen functions of a general vibration problem," *Kungl. Fysiografiska Sällskapets i Lund Förhandlingar*, vol. 21, No. 11 (1951), pp. 1-10.

[14] ———, "Eigenfunction expansions connected with elliptic differential operators," *Proceedings of the 12th Congress of Scandinavia Mathematicians*, Lund, 1954.

[15] ———, *Applications of the theory of direct integrals of Hilbert spaces to some integral and differential operators*, Lecture No. 11, Institute for Fluid Dynamics and Applied Mathematics, University of Maryland, 1954.

[16] I. M. Gelfand, "Abstrakte Funktionen und Lineare Operatoren," *Matematičeskii Sbornik* (N. S.), vol. 4 (1948), pp. 235-284.

[17] I. M. Gelfand and A. G. Kostyucenko, "On expansions in characteristic functions of differential operators and other operators," *Doklady Akademii Nauk SSSR*, vol. 103 (1955), pp. 349-352.

[18] I. M. Gelfand and G. E. Silov, "Quelques applications de la théorie des fonctions généralisées," *Journal de Mathématiques Pures et Appliquées*, vol. 35 (1956), pp. 383-413.

[19] P. R. Halmos, "Normal dilations and extensions of operators," *Summa Brasiliensis Mathematicae*, vol. 2 (1950), pp. 125-134.

[20] L. Hormander, "On the theory of general partial differential operators," *Acta Mathematica*, vol. 94 (1955), pp. 161-248.

[21] Y. Kilpi, "Über lineare normale Transformationen im Hilbertschen Raum," *Annales Academiae Scientiarum Fennicae*, Series A-1, No. 154 (1953), pp. 7-38.

[22] F. I. Mautner, "On eigenfunction expansions," *Proceedings of the National Academy of Sciences*, vol. 39 (1953), pp. 49-53.

[23] B. Sz. Nagy, Appendix to the 3rd Edition of *Leçons d'Analyse Fonctionelle* by F. Riesz and B. Sz. Nagy, Budapest, 1955.

[24] H. Nakano, "Zur Eigenwerttheorie normaler Operatoren," *Proceedings of the Physical-Mathematical Society of Japan*, III Ser., vol. 21 (1939), pp. 315-339.

[25] ———, "Hypermaximalität normaler Operatoren," *ibid.*, III Ser., vol. 22 (1940), pp. 259-264.

[26] A. Ya. Povsner, "On the expansion of arbitrary functions in characteristic functions of the operator $-\Delta + cu$," *Matematičeskii Sbornik*, N. S., vol. 32 (1953), pp. 109-156

[27] F. Riesz and B. Sz. Nagy, *Leçons d'Analyse Fonctionelle*, 3rd Ed., Budapest, 1955.

[28] L. Schwartz, *Théorie des distributions*, Vols. 1 and 2, Paris, 1951.

A GENERAL THEORY OF ALGEBRAIC GEOMETRY OVER DEDEKIND DOMAINS, II.*

Separably Generated Extensions and Regular Local Rings.

By MASAYOSHI NAGATA.

The main aim of the present paper (Chapters 3 and 4) is to prove some preliminary results on separably generated extensions and on regular local rings. We want to remark here that in the present paper we need not assume that the ground rings satisfy the finiteness condition for integral extensions (cf. Part I ([17])).

In Chapter 3, we first prove some results on the notion of tensor product over Dedekind domains (§1), and then we introduce the notions of local and complete tensor products (§2) and derivations of a ring (§3). Making use of these results and notions, we study separably generated extensions and regular extensions (§4). In §5, we prove a generalization of a lemma due to Zariski [25] on regular extensions, and in §6 we treat tensor products of normal rings.

In Chapter 4, we first prove some lemmas on extensions of regular local rings (§1) and on quadratic transformations (§2). In §3, we state some results due to Serre [22] on regular local rings. In §4, we study the notion of unramifiedness of regular local rings and of spots, and in §5, we prove some results on the unique factorization theorem in local rings.

In Appendix 1, we prove that if $\mathfrak{p}$ is a prime ideal of a simple spot P in the restricted case, then $P_{\mathfrak{p}}$ is a simple spot (which is contained in Serre's results) by a similar method as in Zariski [26]. In Appendix 2, we show that the results in Chapter 2 (in Part I) hold good also in the non-restricted case under the assumption that function fields are separably generated. Furthermore, we prove that the completion of a normal spot (in the non-restricted case) in an integral domain.

Terminology.

Terms such as rings, local rings, semi-local rings, normal rings, derived

---

* Received December 16, 1957.

normal rings, rank of rings or ideals, co-rank of ideals and so on are used in the same sense as in Part I ([17]). An integral domain $\mathfrak{o}$ is called a *unique factorization ring* if every element of $\mathfrak{o}$ is expressible, uniquely (up to units), as a product of irreducible elements. In the present paper, spots, affine rings, ground rings and function fields are allowed to be in the *non-restricted case* (see Part I), unless the contrary is explicitly stated. A subring I of a semi-local ring $\mathfrak{o}$ is called a *semi-ground ring* of $\mathfrak{o}$ if 1) I is a field or a Dedekind domain, 2) elements of I are not zero-divisors in $\mathfrak{o}$, and 3) for every maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$, $\mathfrak{o}/\mathfrak{p}$ is a finitely generated field over the field of quotients of $I/(\mathfrak{p} \cap I)$. Observe that if a semi-local ring $\mathfrak{o}$ is a ring of quotients of an affine ring over a ground ring I, then I is a semi-ground ring of $\mathfrak{o}$ and that if I is a semi-ground ring of a semi-local ring $\mathfrak{o}$, then I is also a semi-ground ring of the completion of $\mathfrak{o}$.

Results assumed to be known.

Besides results assumed to be known in Part I, we assume that the following results are known.

1) On the notion of tensor products: Results contained in Bourbaki [1, §§ 1-3].

2) On the theory of fields: Results contained in Weil [24, Chapter I].

3) On the theory of local rings:

LEMMA 0.10 (The structure theorem of complete local rings). *If* $\mathfrak{o}$ *is a complete local ring, then* $\mathfrak{o}$ *has a coefficient ring* $\mathfrak{v}$; *that is,* $\mathfrak{v}$ *is a homomorphic image of a complete discrete valuation ring which satisfies the following conditions:* 1) $\mathfrak{v}$ *is dominated by* $\mathfrak{o}$, 2) *the residue class field of* $\mathfrak{o}$ *coincides with that of* $\mathfrak{v}$, *and* 3) *if* p *is the characteristic of the residue class field of* $\mathfrak{o}$, *then the maximal ideal of* $\mathfrak{v}$ *is generated by* p (*that is,* p *times the identity*). *Then* $\mathfrak{o}$ *is isomorphic to a homomorphic image of a formal power series ring over* $\mathfrak{v}$. (Cohen [6]; for the proof see Narita [20].)[1]

LEMMA 0.11. *If a complete local ring* $\mathfrak{o}$ *is dominated by a local ring* $\mathfrak{o}'$, *then* $\mathfrak{o}$ *is a subspace of* $\mathfrak{o}'$. (See Chevalley [3], Cohen [6], Nagata [15].)

LEMMA 0.12. *Let* $\mathfrak{p}$ *be a prime ideal of a regular local ring* $\mathfrak{r}$. *Then* $\mathfrak{r}/\mathfrak{p}$ *is regular if and only if there exists a regular system of parameters*

---

[1] Cohen's proof is stated also in Samuel [21]. It seems to me that Narita's proof is simpler than the others. The proof in Nagata [11] contains some errors and it is good only in the cases 1) the residue class field is perfect and 2) it contains a field.

$x_1, \cdots, x_n$ ($n = rank$ $\mathfrak{r}$) *such that* $\mathfrak{p} = \sum_1^r x_i\mathfrak{r}$ (*for some* r, *whence* $r = rank$ $\mathfrak{p}$). (See Cohen [6], Nagata [15]; cf. Chevalley [3].)

Remark 1. Let $\mathfrak{o}$ be a local ring of rank r, and let $\mathfrak{m}$ be its maximal ideal. Then elements $u_1, \cdots, u_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ if and only if their residue classes modulo $\mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ over the field $\mathfrak{o}/\mathfrak{m}$. (See Cohen [6], Nagata [15]; cf. [16, § 6].) Therefore, $\mathfrak{o}$ is regular if and only if the dimension of the vector space $\mathfrak{m}/\mathfrak{m}^2$ over $\mathfrak{o}/\mathfrak{m}$ is equal to the rank of $\mathfrak{o}$.

Remark 2. Let $\mathfrak{o}$ be a local ring, and let $\mathfrak{p}$ be an ideal of rank r. If $\mathfrak{p}$ is generated by r elements and if $\mathfrak{o}/\mathfrak{p}$ is regular, then $\mathfrak{o}$ is a regular local ring, as is easily seen.

LEMMA 0.13. *A complete local ring* $\mathfrak{o}$ *is a Henselian ring, that is, if a monic polynomial* $f(x)$ *over* $\mathfrak{o}$ *factors into a product of monic polynomials* $g(x)$ *and* $h(x)$ *modulo the maximal ideal* $\mathfrak{m}$ *of* $\mathfrak{o}$, *and if*

$$g(x)\mathfrak{o}[x] + h(x)\mathfrak{o}[x] + \mathfrak{m}[x] = \mathfrak{o}[x],$$

then there exist monic polynomials $g'(x)$ *and* $h'(x)$ $(\in \mathfrak{o}[x])$ *such that* $f(x) = g'(x)h'(x)$ *and both* $g(x) - g'(x)$ *and* $h(x) - h'(x)$ *are in* $\mathfrak{m}[x]$. (See Cohen [6], Nagata [11], Samuel [21].)

LEMMA 0.14. *Let* $\mathfrak{o}$ *be a complete local ring, not necessarily Noetherian. If the maximal ideal of* $\mathfrak{o}$ *has a finite base, then* $\mathfrak{o}$ *is Noetherian.* (See Cohen [6], Nagata [15], Samuel [21].)

Further, only in Chapter 4, §§ 3-5, the results on regular local rings contained in Serre [22] are assumed to be known (and they are listed in Chapter 4, § 3.)

4) On Noetherian integral domains:

Some results stated in Nagata [19] will be used freely; in particular, we shall use the following

LEMMA 0.15. *Let* $\mathfrak{o}$ *be a Noetherian integral domain of rank* 1, *and let* K *be a finite algebraic extension of the field of quotients of* $\mathfrak{o}$. *If a subring* $\mathfrak{o}'$ *of* K *contains* $\mathfrak{o}$, *then* $\mathfrak{o}'$ *is a Noetherian ring* (*of rank not greater than* 1). *Further, in this case, if* $\mathfrak{p}'$ *is a prime ideal of* $\mathfrak{o}'$ *different from* 0, *then* $\mathfrak{o}'/\mathfrak{p}'$ *is a finite algebraic extension of* $\mathfrak{o}/(\mathfrak{p}' \cap \mathfrak{o})$. (Akizuki; cf. Chevalley [5], Cohen [7].)

5) On homological algebras:

Some basic notions and results contained in Cartan-Eilenberg [2] are assumed to be known (only in Chapter 4, §§ 3-5).

Chapter 3. Separably Generated Extensions.

1. Preliminaries on the notion of tensor products. Let I be a ring, and let M and N be I-modules. Then, as is well known, we can define the tensor product of M and N over I, which will be denoted by $M \otimes_I N$ or by $M \otimes N$; if M and N are rings, then $M \otimes N$ becomes a ring.

LEMMA 1. *Let I be a subring of a ring $\mathfrak{o}$. If S is a multiplicatively closed subset of I which does not contain 0, then $\mathfrak{o} \otimes_I I_S$ can be identified with $\mathfrak{o}_S$.*

The proof consists in remarking that by the definition of the ring of quotients (see [16, § 2]) and the tensor product, both $\mathfrak{o}_S$ and $\mathfrak{o} \otimes I_S$ are characterized by the property of being the most "universal" ring in which the elements of S are mapped on units and which is generated by images of $\mathfrak{o}$ and inverses of images of elements of S.

LEMMA 2. *If $\mathfrak{o}$, $\mathfrak{o}'$ and I' are rings containing a common subring I, then $(\mathfrak{o} \otimes_I \mathfrak{o}') \otimes_I I'$ can be identified with $(\mathfrak{o} \otimes_I I') \otimes_{I'} (\mathfrak{o}' \otimes_I I')$. If furthermore, I' is a subring of $\mathfrak{o}'$, then $\mathfrak{o} \otimes_I \mathfrak{o}'$ can be identified with $(\mathfrak{o} \otimes_I I') \otimes_{I'} \mathfrak{o}'$.*[2]

The proof is easy; see [1, § 3, Exercise 4) and No. 4].

Let I be an integral domain. We say that an I-module M is torsion-free if $am = 0$ $(a \in I,\ m \in M)$ implies $a = 0$ or $m = 0$. An I-module which is not torsion-free is said to have torsion. Now we shall state the following well known lemma:

LEMMA 3. *Assume that I is a principal ideal integral domain and that M is a finite I-module. If M is torsion-free, then M has a linearly independent base.*

PROPOSITION 1. *Assume that I is a Dedekind domain. If I-modules M and N are torsion-free, then $M \otimes N$ is also torsion free.*

Proof.[3] If $M \otimes N$ has torsion, then there exist submodules M' and N' of M and N respectively which are finite modules such that $M' \otimes N'$ has torsion (see [1]). Therefore, we may assume that M and N are finite modules. Then, defining multiplication in M and N so that $M^2 = N^2 = 0$, we construct rings $I+M$ and $I+N$ (direct sums as modules). Then $M\otimes N$ is imbedded in $(I+M)\otimes(I+N)$ (see [1]), and this last ring is Noetherian because M and N are finitely generated. Let $\mathfrak{p}^*_1,\cdots,\mathfrak{p}^*_h$ be the prime divisors of zero in $(I+M)\otimes(I+N)$ and set $\mathfrak{p}_i=\mathfrak{p}^*_i\cap I$ for each i. Let S be the intersection of the complements of the $\mathfrak{p}_i$'s in I. Then for an element $a\in S$, $su=0$ $(u\in(I+M)\otimes(I+N))$ implies $u=0$. Therefore, $(I+M)\otimes(I+N)$ can be imbedded in $(I_S+(M\otimes I_S))\otimes_{I_S}(I_S+(N\otimes I_S))$. Therefore, in particular, $M\otimes N$ can be imbedded in $(M\otimes I_S)\otimes_{I_S}(N\otimes I_S)$. Thus we may assume that I is a semi-local Dedekind domain. Then I is a principal ideal ring (see [16, § 9]), and M and N have linearly independent bases by Lemma 3. Therefore $M\otimes N$ is torsion-free (see [1]).

---

[2] In general, I' may not be identified with the subring $1 \otimes I'$ of $\mathfrak{o} \otimes I'$. Of course, if I is a field, the identification is permissible.

[3] Another proof can be given making use of the following fact: If a finite I-module M is torsion-free, then M is isomorphic to the direct sum of a finite number of ideals of I and M is a projective module. (For the notion of projective module, see [2].)

COROLLARY. *Let $\mathfrak{o}$ and $\mathfrak{s}$ be rings containing a Dedekind domain I, and let S be the set of all non-zero elements of I. If every element of S is not a zero-divisor in both $\mathfrak{o}$ and $\mathfrak{s}$, then $\mathfrak{o}\otimes_I\mathfrak{s}$ can be imbedded in $\mathfrak{o}_S\otimes_{I_S}\mathfrak{s}_S$.*

The proof is immediate from Lemma 1 and Proposition 1.

Remark. As is well known, we can identify $\mathfrak{o}\otimes 1$ and $1\otimes\mathfrak{s}$ with $\mathfrak{o}$ and $\mathfrak{s}$ respectively (in the above case). Then $\mathfrak{o}\otimes_I\mathfrak{s}$ is the subring of $\mathfrak{o}_S\otimes_{I_S}\mathfrak{s}_S$ generated by $\mathfrak{o}$ and $\mathfrak{s}$. This identification will be made in every similar case.

THEOREM 1. *Let $\mathfrak{o}$ and $\mathfrak{s}$ be integral domains which contain a Dedekind domain I. Let K, L and $\boldsymbol{k}$ be the fields of quotients of $\mathfrak{o}$, $\mathfrak{s}$ and I respectively. Then $\mathfrak{o}\otimes_I\mathfrak{s}$ is the subring of $K\otimes_{\boldsymbol{k}}L$ generated by $\mathfrak{o}$ and $\mathfrak{s}$. Furthermore, $\mathfrak{o}\otimes\mathfrak{s}$ and $K\otimes L$ have the same total quotient ring, and therefore $K\otimes L$ is an integral domain if and only if $\mathfrak{o}\otimes\mathfrak{s}$ is.*

Proof. By the corollary to Proposition 1, $\mathfrak{o}\otimes\mathfrak{s}$ is the subring of $\mathfrak{o}_S\otimes_{\boldsymbol{k}}\mathfrak{s}_S$ generated by $\mathfrak{o}$ and $\mathfrak{s}$, S being the set of non-zero elements of I. Since $\boldsymbol{k}$ is a field, $\mathfrak{o}_S\otimes_{\boldsymbol{k}}\mathfrak{s}_S$ is a subring of $K\otimes_{\boldsymbol{k}}L$, which proves the first assertion. From this fact, we see that elements of $\mathfrak{o}$ and $\mathfrak{s}$ are not zero-divisors in $\mathfrak{o}\otimes\mathfrak{s}$. Therefore the total quotient ring A of $\mathfrak{o}\otimes\mathfrak{s}$ contains K and L and therefore also $K\otimes L$, which proves the last assertion.

LEMMA 4. *Let $\mathfrak{o}$ and $\mathfrak{s}$ be rings which contain a ring I. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathfrak{o}$ and $\mathfrak{s}$ respectively, and assume that $\mathfrak{a}\cap I=\mathfrak{b}\cap I$. Denote by I' the ring $I/(\mathfrak{c}\cap I)$ and by $\mathfrak{d}$ the ideal of $\mathfrak{o}\otimes\mathfrak{s}$ generated by $\mathfrak{a}$ and $\mathfrak{b}$. Then $(\mathfrak{o}\otimes_I\mathfrak{s})/\mathfrak{d}$ can be identified with $(\mathfrak{o}/\mathfrak{a})\otimes_{I'}(\mathfrak{s}/\mathfrak{b})$.*

This is well known and we shall omit the proof (see [1]).

LEMMA 5. *Let K be a ring of quotients of an affine ring over a ground* *ring I, and let L be a Noetherian integral domain containing I. Then $K \otimes_I L$ is a Noetherian ring and its zero ideal has no imbedded prime divisor.*

Proof. Since $K \otimes L$ is a ring of quotients of a finitely generated ring over the Noetherian ring L, we see that $K \otimes L$ is Noetherian. In order to prove the last assertion, we may assume that K, L and I are fields by Theorem 1. Let $x_1, \cdots, x_n$ be a transçendence base of K over I, and let L' be the field of quotients of $I(x_1, \cdots, x_n) \otimes_I L$; since the x_i's are algebraically independent over L, $L' = L(x_1, \cdots, x_n)$. Since I is a field, $K \otimes L$ is a subring of $K \otimes_{I'} L'$, where I' denotes the field $I(x_1, \cdots, x_n)$. *Now* we see our assertion easily, because K is a finite alegbraic extension of I' and $K \otimes_{I'} L'$ has minimum condition.

2. Local tensor product and complete tensor product. Let $\mathfrak{o}$ and $\mathfrak{o}'$ be semi-local rings and assume that I is a subring of them. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be maximal ideals of $\mathfrak{o}$ and $\mathfrak{o}'$ respectively, and set $\mathfrak{q} = \mathfrak{p} \cap I$, $\mathfrak{q}' = \mathfrak{p}' \cap I$. We assume that $I/\mathfrak{q}$ is a field or a Dedekind domain and that $\mathfrak{o}/\mathfrak{p}$ is a function field over $I/\mathfrak{q}$ for every maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$. Set $\mathfrak{t} = \mathfrak{o} \otimes_I \mathfrak{o}'$. Then we have

Lemma 1. *$\mathfrak{p}\mathfrak{t} + \mathfrak{p}'\mathfrak{t} \neq \mathfrak{t}$ if and only if $\mathfrak{q} = \mathfrak{q}'$. In this case,* 1) *$\mathfrak{t}/(\mathfrak{p}\mathfrak{t} + \mathfrak{p}'\mathfrak{t})$ is Noetherian,* 2) *every prime divisor $\mathfrak{P}$ of $\mathfrak{p}\mathfrak{t} + \mathfrak{p}'\mathfrak{t}$ is a minimal prime divisor, and* 3) *$\mathfrak{P}$ has a finite base.*

Proof. The first assertion is obvious because $\mathfrak{p}$ and $\mathfrak{p}'$ are maximal. 1) and 2) follow from Lemmas 3.1.4 and 3.1.5. Since $\mathfrak{p}$ and $\mathfrak{p}'$ have finite bases, 3) follows from 1).

Now, let S be the intersection of the complements of prime divisors of $\mathfrak{p}\mathfrak{t} + \mathfrak{p}'\mathfrak{t}$, where $\mathfrak{p}$ and $\mathfrak{p}'$ run over all possible maximal ideals. Then $\mathfrak{t}_S$ is called the local tensor product of $\mathfrak{o}$ and $\mathfrak{o}'$ over I; this ring will be denoted by $\mathfrak{o} \times_I \mathfrak{o}'$ or by $\mathfrak{o} \times \mathfrak{o}'$. By this definition, $\mathfrak{o} \times \mathfrak{o}'$ is a semi-local ring if it is Noetherian.

Lemma 2. *If I is a semi-ground ring of $\mathfrak{o}$ and if $\mathfrak{o}'$ is torsion-free as an I-module, then $\mathfrak{o} \times \mathfrak{o}'$ is also torsion-free. If, furthermore, I is a semi-ground ring of $\mathfrak{o}'$ and if $\mathfrak{o} \times \mathfrak{o}'$ is a semi-local ring, then I is also a semi-ground ring of $\mathfrak{o} \times \mathfrak{o}'$.*

Proof. By the Corollary to Proposition 1, we see that $\mathfrak{o} \otimes \mathfrak{o}'$ is torsion-free. Since $\mathfrak{o} \times \mathfrak{o}'$ is a ring of quotients of $\mathfrak{o} \otimes \mathfrak{o}'$, we see the validity of the first assertion (see [16, § 2]). Now the last assertion is obvious.

Under the same assumptions and notations as in Lemma 2, let $\mathfrak{m}$ be the J-radical of $\mathfrak{o} \times \mathfrak{o}'$ and set $\mathfrak{n} = \bigcap_n \mathfrak{m}^n$. Then $(\mathfrak{o} \times \mathfrak{o}')/\mathfrak{n}$ is a semi-local ring which may not be Noetherian. The completion of this semi-local ring is called the complete tensor product of $\mathfrak{o}$ and $\mathfrak{o}'$ (over I) and will be denoted by $\mathfrak{o} \bar{\otimes}_I \mathfrak{o}'$, or by $\mathfrak{o} \bar{\otimes} \mathfrak{o}'$. Observe that $\mathfrak{o} \otimes \mathfrak{o}'$ is the limit space of the inverse system $\{(\mathfrak{o} \times \mathfrak{o}')/\mathfrak{m}^n;\ n = 1, 2, \cdots\}$.

LEMMA 3. *$\mathfrak{o} \bar{\otimes} \mathfrak{o}'$ is a (Noetherian) semi-local ring.*

Proof. By Lemma 1, every maximal ideal of $\mathfrak{o} \times \mathfrak{o}'$ has a finite base and the same is true of $\mathfrak{o} \bar{\otimes} \mathfrak{o}'$. Therefore $\mathfrak{o} \bar{\otimes} \mathfrak{o}'$ is Noetherian by Lemma 0.14.

LEMMA 4. *Let $\mathfrak{o}^*$ and $\mathfrak{o}'^*$ be semi-local rings which contain $\mathfrak{o}$ and $\mathfrak{o}'$ as dense subspaces respectively. Then $\mathfrak{o}^* \bar{\otimes} \mathfrak{o}'^* = \mathfrak{o} \bar{\otimes} \mathfrak{o}'$.*

Proof. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the J-radicals of $\mathfrak{o}$ and $\mathfrak{o}'$ respectively. Then $\mathfrak{m}\mathfrak{o}^*$ and $\mathfrak{m}\mathfrak{o}'^*$ are the J-radicals of $\mathfrak{o}^*$ and $\mathfrak{o}'^*$ respectively. Let $\mathfrak{a}(n)$ be the ideal of $\mathfrak{o} \bar{\otimes} \mathfrak{o}'$ generated by $\mathfrak{m}^n$ and $\mathfrak{m}'^n$ and let $\mathfrak{a}$ be the J-radical of $\mathfrak{o} \otimes \mathfrak{o}'$. Then we see that $\mathfrak{a}(1)$ contains a power of $\mathfrak{a}$ by Lemma 1. On the other hand, it is obvious that $\mathfrak{a}(1)^{2n} \subseteq \mathfrak{a}(n) \subseteq \mathfrak{a}(1)^n$. Therefore $\mathfrak{o} \bar{\otimes} \mathfrak{o}'$ can be identified with the limit space of the inverse system

$$\{(\mathfrak{o} \times \mathfrak{o}')/(\mathfrak{m}^n(\mathfrak{o} \times \mathfrak{o}') + \mathfrak{m}'^n(\mathfrak{o} \times \mathfrak{o}'))\}.$$

Similarly, $\mathfrak{o}^* \bar{\otimes} \mathfrak{o}'^*$ can be identified with the limit space of the inverse system

$$\{(\mathfrak{o}^* \times \mathfrak{o}'^*)/(\mathfrak{m}^n(\mathfrak{o}^* \times \mathfrak{o}'^*) + \mathfrak{m}'^n(\mathfrak{o}^* \times \mathfrak{o}'^*))\}.$$

Since

$$\begin{aligned}(\mathfrak{o}^* \times \mathfrak{o}'^*)/(\mathfrak{m}^n(\mathfrak{o}^* \times \mathfrak{o}'^*) &+ \mathfrak{m}'^n(\mathfrak{o}^* \times \mathfrak{o}'^*)) \\ &= (\mathfrak{o}^*/\mathfrak{m}^n\mathfrak{o}^*) \times (\mathfrak{o}'^*/\mathfrak{m}'^n\mathfrak{o}'^*) = (\mathfrak{o}/\mathfrak{m}^n) \times (\mathfrak{o}'/\mathfrak{m}'^n) \\ &= (\mathfrak{o} \times \mathfrak{o}')/(\mathfrak{m}^n(\mathfrak{o} \times \mathfrak{o}') + \mathfrak{m}'^n(\mathfrak{o} \times \mathfrak{o}')),\end{aligned}$$

we have $\mathfrak{o} \otimes \mathfrak{o}' = \mathfrak{o}^* \bar{\otimes} \mathfrak{o}'^*$.

Remark. The notion of complete tensor product of complete local rings over a field was introduced by Chevalley [4], who called it the *Kronecker product.* Though his formulation is different from ours, if we restrict ourselves to his case, then the two definitions are essentially the same: If $\mathfrak{o}$ and $\mathfrak{o}'$ are complete local rings which have basic fields $\boldsymbol{k}$ and $\boldsymbol{k}'$ respectively (for the definition of basic fields in Chevalley's sense, see [3]), and if M is a field containing both $\boldsymbol{k}$ and $\boldsymbol{k}'$, then the Kronecker product of $\mathfrak{o}$ and $\mathfrak{o}'$ over M is $(\mathfrak{o}' \bar{\otimes}_{\boldsymbol{k}} M) \otimes_M (\mathfrak{o}' \bar{\otimes}_{\boldsymbol{k}'} M)$. (This fact can be proved using some results in [4] and a method similar to the proof of Lemma 4.)

3. Derivations of a ring. A *derivation* D of a ring $\mathfrak{o}$ is an additive endomorphism of the total quotient ring L of $\mathfrak{o}$ which satisfies the following conditions: 1) $D(xy)=xDy+yDx$ for $x,y\in L$ and 2) there exists an element d of $\mathfrak{o}$ which is not a zero-divisor such that $dDx\in\mathfrak{o}$ for $x\in\mathfrak{o}$.

Here, if d can be chosen to be 1, then we call D an *integral derivation* of $\mathfrak{o}$.

Let D be a derivation of $\mathfrak{o}$ and let $\mathfrak{o}'$ be a subring of $\mathfrak{o}$. If $Da=0$ for every $a\in\mathfrak{o}'$, then we say that D is a derivation *over* $\mathfrak{o}'$; if $Da=0$ for every $a\in\mathfrak{o}$, then we say that D is the zero derivation or the trivial derivation of $\mathfrak{o}$, which will be denoted by 0.

Remark 1. Since $1^2=1$, $D1=D1+D1$ and $D1=0$ for every derivation D of $\mathfrak{o}$. Therefore every derivation of $\mathfrak{o}$ is a derivation over the subring of $\mathfrak{o}$ generated by the identity.

Remark 2. If $x,y\in\mathfrak{o}$ and if y is not a zero-divisor, then $D(x/y)=(yDx-xDy)/y^2$. (For, since $x=(x/y)y$, $Dx=yD(x/y)+(x/y)Dy$ and $D(x/y)=(yDx-xDy)/y^2$.) Therefore, if D is a derivation over a subring $\mathfrak{o}'$ of $\mathfrak{o}$ and if S is the set of elements of $\mathfrak{o}'$ which are not zero-divisors in $\mathfrak{o}$, then $Da=0$ for every element a of $\mathfrak{o}'_S$.

The set of derivations of $\mathfrak{o}$ over a subring $\mathfrak{o}'$ is an $\mathfrak{o}$-module. Linear dependence of derivations will always mean dependence in this module, hence over $\mathfrak{o}$.

Let $\mathfrak{o}$ be a ring and let $X_1,\cdots,X_n$ be indeterminates. Then there exist derivations D_i $(i=1,\cdots,n)$ of $\mathfrak{o}[X_1,\cdots,X_n]$ over $\mathfrak{o}$ such that $D_iX_i=1$ and $D_iX_j=0$ if $i\neq j$. These D_i are called the partial derivations and will be denoted by $\partial/\partial X_i$ (if $f\in\mathfrak{o}[X_1,\cdots,X_n]$, then D_if may be denoted by $\partial f/\partial X_i$). When $f_1,\cdots,f_r$ are elements of $\mathfrak{o}[X_1,\cdots,X_n]$, the matrix $(\partial f_i/\partial X_j)$ is called the Jacobian matrix of $f_1,\cdots,f_r$ and will be denoted by $J(f_1,\cdots,f_r)$.

Let D be a derivation of $\mathfrak{o}$. Then there exists a uniquely determined derivation D' of $\mathfrak{o}[X_1,\cdots,X_n]$ which coincides with D on $\mathfrak{o}$ and $D'X_i=0$. If f is in the total quotient ring of $\mathfrak{o}[X_1,\cdots,X_n]$, $D'f$ is denoted by f^D.

Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}[X_1,\cdots,X_n]$, and let S be the intersection of the complements of all prime ideals which are prime divisors of $\mathfrak{a}$ or of zero. Let ϕ be the natural homomorphism from $\mathfrak{o}[X_1,\cdots,X_n]_S$ into the total quotient ring of $\mathfrak{o}[X_1,\cdots,X_n]/\mathfrak{a}$ and set $x_i=\phi(X_i)$. When $f\in\mathfrak{o}[X_1,\cdots,X_n]_S$, $\phi(\partial f/\partial X_i)$ will be denoted by $\partial f/\partial x_i$. If D is a derivation of $\mathfrak{o}$ and there exists an element $d\in S\cap\mathfrak{o}$ such that dD is an integral derivation, $\phi(f^D)$ will be denoted by $f^D(x_1,\cdots,x_n)$ for every element $f=f(X_1,\cdots,X_n)$ of $\mathfrak{o}[X_1,\cdots,X_n]_S$.

Remark 1. $\partial/\partial X_1, \cdots, \partial/\partial X_n$ form a maximal linearly independent set of derivations of $\mathfrak{o}[X_1, \cdots, X_n]$ over $\mathfrak{o}$.

Remark 2. If D is a derivation of $\mathfrak{o}[X_1, \cdots, X_n]/\mathfrak{a}$ over $\phi(\mathfrak{o})$, then for an element g of $\mathfrak{o}[X_1, \cdots, X_n]$, $D(\phi(g)) = \sum Dx_i \cdot (\partial g/\partial x_i)$.

LEMMA 1. *Let $\boldsymbol{k}$ be a field with a derivation D and let $X_1, \cdots, X_n$ be indeterminates. Set $R = \boldsymbol{k}[X_1, \cdots, X_n]$ and let $\mathfrak{p}$ be a prime ideal of R with a base $f_1, \cdots, f_s$ and let L be the field of quotients of $R/\mathfrak{p}$. Then there exists a derivation D' of L such that* 1) *D' coincides with D on $\boldsymbol{k}$ and* 2) *$D'x_i = u_i$ (where x_i is the class of X_i modulo $\mathfrak{p}$ and $u_i \in L$) if and only if $u_1, \cdots, u_n$ satisfy the following set of linear equations:*

$$f_i^D(x_1, \cdots, x_n) + \sum(\partial f_i/\partial x_j)u_j = 0.$$

In this case, D' is uniquely determined.

For the proof, see Weil [24].

COROLLARY. *Let r be the rank of the Jacobian matrix $J(f_1, \cdots, f_s)$ modulo $\mathfrak{p}$. Then every maximal linearly independent set of derivations of L over $\boldsymbol{k}$ consists of $n - r$ elements.* (See Weil [24].)

LEMMA 2. *Let L be a function field over a ground field $\boldsymbol{k}$ of characteristic p.* 1) *If $\dim L = r$, then there exists at least r linearly independent derivations of L over $\boldsymbol{k}$; L has no more than r linearly independent derivations over $\boldsymbol{k}$ if and only if L has a separating transcendence base over $\boldsymbol{k}$.* 2) *Assume that $p \neq 0$ and that a is an element of $\boldsymbol{k}$ such that $a^{1/p} \notin \boldsymbol{k}$. Then there exists a derivation D of $\boldsymbol{k}(a^{1/p})$ over $\boldsymbol{k}$ such that $D(a^{1/p}) = 1$; every derivation of $\boldsymbol{k}(a^{1/p})$ over $\boldsymbol{k}$ is of the form xD with $x \in \boldsymbol{k}(a^{1/p})$.*

For the proof, see Weil [24].

PROPOSITION 2. *Let $\mathfrak{o}$ be an integral domain finitely generated over a ring I and let $\boldsymbol{k}$ and L be the fields of quotients of I and $\mathfrak{o}$ respectively. Then an additive endomorphism D of L is a derivation of $\mathfrak{o}$ over I if and only if D is a derivation of L over $\boldsymbol{k}$; in this case, D is a derivation of an arbitrary ring of quotients of $\mathfrak{o}$.*

Proof. If D is a derivation of $\mathfrak{o}$, then D is a derivation of L by definition; if D is a derivation over I, then by Remark 2 after the definition, we see that D is a derivation over $\boldsymbol{k}$. Conversely, assume that D is a derivation of L over $\boldsymbol{k}$. Let $x_1, \cdots, x_n$ be elements of $\mathfrak{o}$ such that $\mathfrak{o} = I[x_1, \cdots, x_n]$ and let S be a multiplicately closed subset of $\mathfrak{o}$ which does not contain zero.

Let d $(\neq 0)$ be an element of $\mathfrak{o}$ such that $dDx_i \in \mathfrak{o}$ for every i. Then, since every element y of $\mathfrak{o}$ is expressed as a polynomial in x_i's ,we have $dDy \in \mathfrak{o}$. Then for an element $z = y/s$ $(y \in \mathfrak{o}, s \in S)$, $Dz = (sDx - xDs)/s^2$ and we have $dDz \in \mathfrak{o}_S$. Thus the proof is completed.

Let $\mathfrak{a}$ be an ideal of a ring $\mathfrak{o}$ and let D be a derivation of $\mathfrak{o}$. Let ϕ be the natural homomorphism from $\mathfrak{o}$ onto $\mathfrak{o}/\mathfrak{a}$. Assume that there exists an element d of $\mathfrak{o}$ which is not a zero-divisor modulo $\mathfrak{a}$ and such that dD is an integral derivation of $\mathfrak{o}$ and $dDa \in \mathfrak{a}$ for every element $a \in \mathfrak{a}$. Then we can define an operator D' to be $D'(\phi(x)) = \phi(dDx)/\phi(d)$. Then

LEMMA 3. *D' can be extended uniquely to a derivation of $\mathfrak{o}/\mathfrak{a}$.*

The derivation obtained above is called the derivation *induced* on $\mathfrak{o}/\mathfrak{a}$ by D (observe that D' is independent of the choice of d).

Proof. Let x/y be an element of the total quotient ring of $\mathfrak{o}/\mathfrak{a}$ $(x, y \in \mathfrak{o}/\mathfrak{a})$. Then we define $D^*(x/y) = (yD'x - xD'y)/y^2$. Then it is seen that D^* is a derivation $\mathfrak{o}/\mathfrak{a}$. The uniqueness is obvious because any extension of D' must satisfy the defining property of D^*.

4. Separably generated extensions and regular extensions. We say that a field L is *separably generated* over a subfield $\boldsymbol{k}$ if either $\boldsymbol{k}$ *is* of characteristic 0 or $L \otimes_k \boldsymbol{k}^{1/p}$ is an integral domain, where p is the characteristic of $\boldsymbol{k}$. We say that L is a *regular extension* of $\boldsymbol{k}$ if L is separably generated over $\boldsymbol{k}$ and if $\boldsymbol{k}$ is algebraically closed in L. Then the following three lemmas are well known (see Weil [24]).

LEMMA 1. *L is separably generated over $\boldsymbol{k}$ if and only if every subfield of L which is finitely generated over $\boldsymbol{k}$ has a separating transcendence base. When L is finitely generated over $\boldsymbol{k}$, L is separably generated if and only if L has a separating transcendence base.*

LEMMA 2. *L is separably generated over $\boldsymbol{k}$ if and only if $L \otimes_k K$ is an integral domain for every field K which contains $\boldsymbol{k}$ and in which $\boldsymbol{k}$ is separably algebraically closed.*

LEMMA 3. *The following three conditions for the field L are equivalent to each other:*

1) *L is a regular extension of $\boldsymbol{k}$.*

2) *$L \otimes_k K$ is an integral domain for every field K containing $\boldsymbol{k}$.*

3) *$L \otimes_k K$ is an integral domain for every finite algebraic extension of $\boldsymbol{k}$.*

We say that an integral domain $\mathfrak{o}$ is *separably generated* over a subring I if the field of quotients of $\mathfrak{o}$ is separably generated over that of I; we say that $\mathfrak{o}$ is a *regular extension* of I if the field of quotients of $\mathfrak{o}$ is a regular extension of that of I. When a subset T of $\mathfrak{o}$ forms a separating transcendence base of the field of quotients of $\mathfrak{o}$ over that of I, we say that T is a *separating transcendence base* of $\mathfrak{o}$ over I.

Now we shall treat the case where I is a field or a Dedekind domain. Let $\boldsymbol{k}$ be the field of quotients of I. We denote by p either the number 1 or the characteristic of I according as this characteristic is zero or not. By definition, by Theorem 1 and by Lemmas 1-3, we have immediately the following two theorems.

THEOREM 2. *Let* $\mathfrak{o}$ *be an integral domain which contains the ring* I *(which is a field or a Dedekind domain). Then the following four conditions are equivalent to each other:*

1) $\mathfrak{o}$ *is separably generated over* I.

2) *If* $\mathfrak{s}$ *is an affine ring over* I *contained in* $\mathfrak{o}$, *then* $\mathfrak{s}$ *has a separating transcendence base over* I.

3) *For a fixed natural number* m, $\mathfrak{o}\otimes_I I^{1/p^m}$ *is an integral domain. (This condition may be separated into infinitely many conditions with* $m=1,2,\cdots$.*)*

4) *If* $\boldsymbol{k}$ *is separably algebraically closed in a field* K, *then* $\mathfrak{o}\otimes_I K$ *is an integral domain.*

THEOREM 3. *With the same* $\mathfrak{o}$ *as above, the following four conditions are equivalent to each other:*

1) $\mathfrak{o}$ *is a regular extension of* I.

2) $\mathfrak{o}\otimes_I I'$ *is an integral domain for every finite integral extension* I' *of* I.

3) *If* $\mathfrak{s}$ *is an integral domain containing* I, $\mathfrak{o}\otimes_I\mathfrak{s}$ *is an integral domain.*

4) $\mathfrak{o}$ *is separably generated over* I *and* $\boldsymbol{k}$ *is algebraically closed in the field of quotients of* $\mathfrak{o}$.

COROLLARY 1. *Assume that an integral domain* $\mathfrak{o}$ *is a regular extension of the ring* I. *If* K *is an integral domain containing* I, *then* $\mathfrak{o}\otimes_I K$ *is a regular extension of* K.

Proof. By the definition of regularity and by Theorem 1, we may assume that K is a field. Let L be an arbitrary field containing K. Then

$(\mathfrak{o} \otimes_I K) \otimes_K L = \mathfrak{o} \otimes_I L$ by Lemma 3.1.2. Since $\mathfrak{o}$ is a regular extension of I, $\mathfrak{o} \otimes_I L$ is an integral domain, which shows that $\mathfrak{o} \otimes K$ is a regular extension of K.

COROLLARY 2. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be integral domains which contain the ring I. If $\mathfrak{o}$ and $\mathfrak{o}'$ are regular extensions of I, then $\mathfrak{o} \otimes_I \mathfrak{o}'$ is also a regular extension of I.*

Proof. Let K be a field containing I. Then

$$(\mathfrak{o} \otimes \mathfrak{o}') \otimes K = (\mathfrak{o} \otimes K) \otimes_K (\mathfrak{o}' \otimes K)$$

by Lemma 3.1.2. Since $\mathfrak{o} \otimes K$ and $\mathfrak{o}' \otimes K$ are regular extensions of K by Corollary 1, we see that $(\mathfrak{o} \otimes \mathfrak{o}') \otimes K$ is an integral domain, which proves our assertion.

PROPOSITION 3. *Let $\mathfrak{o}$ be an integral domain finitely generated over a ring I which is not necessarily a Dedekind domain, and let ϕ be a homomorphism from $I[x_1, \cdots, x_n]$ onto $\mathfrak{o}$, where $x_1, \cdots, x_n$ are algebraically independent elements over I. If $\mathfrak{p}$ is the kernel of ϕ and if $f_1, \cdots, f_m$ is a base of $\mathfrak{p}$, then the rank r of the Jacobian matrix $J(f_1, \cdots, f_m)$ modulo $\mathfrak{p}$ is not greater than the rank s of $\mathfrak{p}$; $r = s$ if and only if $\mathfrak{o}$ is separably generated.*

Proof. We may assume that I is a field. Then the assertion follows from the Corollary to Lemma 3.3.1 and Lemma 1.

PROPOSITION 4. *Let $x_1, \cdots, x_n$ be algebraically independent elements over an integral domain I of characteristic $p \neq 0$. Let $\mathfrak{a}$ be an ideal of $I[x_1, \cdots, x_n]$ with $\mathfrak{a} \cap I = 0$ and let $\boldsymbol{k}$ be the field of quotients of I. Assume that $\mathfrak{a}\boldsymbol{k}[x_1, \cdots, x_n]$ is of rank r. Then there exist elements $y_1, \cdots, y_n \in I[x_1, \cdots, x_n]$ and an element a $(\neq 0) \in I$ such that*

1) *$I[1/a, x_1, \cdots, x_n]$ is integral over $I[1/a, y_1, \cdots, y_n]$,*

2) *$\mathfrak{a} \cap I[1/a, y_1, \cdots, y_n]$ is generated by $y_1, \cdots, y_r$ and*

3) *for every derivation D of $I[x_1, \cdots, x_n]$, $Dy_j = Dx_j$ for $j = r+1, \cdots, n$.*

Proof. By Remark 2 after Lemma 1.1.1, we see that the y_i's in Corollary 1 to Proposition 1.1 can be chosen so that $y_j - x_j$ is in $\pi[x_1^p, \cdots, x_r^p]$ for $j = r+1, \cdots, n$, where π denotes the prime integral domain. In this case, the y_i are the required elements.

THEOREM 4. (NORMALIZATION THEOREM FOR SEPARABLY GENERATED INTEGRAL DOMAINS) *Let* $\mathfrak{o}$ *be an integral domain finitely generated over a subring* I. *If* $\mathfrak{o}$ *is separably generated over* I, *then there exist a separating transcendence base* $z_1, \cdots, z_t$ *of* $\mathfrak{o}$ *over* I *and an element* a $(\neq 0)$ *of* I *such that* $\mathfrak{o}[1/a]$ *is integral over* $I[1/a, z_1, \cdots, z_t]$.

Proof. When I is of characteristic zero, our assertion is nothing but the normalization theorem (Corollary 2 to Proposition 1.1). Therefore we assume that I is of characteristic $p \neq 0$. Let $D_1, \cdots, D_t$ be a maximal linearly independent set of derivations of $\mathfrak{o}$ over I. Then $t =$ transcendence degree of $\mathfrak{o}$ over I by Lemma 3.3.2. Take elements $y_1, \cdot\cdot, y_t$ of $\mathfrak{o}$ such that $D_i y_j \neq 0$ if and only if $i = j$. Let $w_1, \cdots, w_s$ be elements of $\mathfrak{o}$ such that $\mathfrak{o} = I[w_1, \cdots, w_s, y_1, \cdots, y_t]$ and apply the proof of Proposition 4; we see that the z_i's in Corollary 2 to Proposition 1.1 can be selected so that $y_i - z_i \in \pi[w_1{}^p, \cdots, w_s{}^p]$ (π being the prime integral domain of I). Then for every derivation D of $\mathfrak{o}$, $Dy_i = Dz_i$. Therefore, in particular, $D_i z_j \neq 0$ if and only if $i = j$. Let D be an arbitrary derivation of $\mathfrak{o}$ over $I[z_1, \cdots, z_t]$. Then there are elements f $(\neq 0)$, $f_1, \cdots, f_t \in \mathfrak{o}$ such that $fD = \sum f_i D_i$ (because D is a derivation of $\mathfrak{o}$ over I). Then $0 = fDz_j = f_j D_j z_j$, $f_j = 0$ for every j, and $D = 0$. Thus we see that $\mathfrak{o}$ is separably algebraic over $I[z_1, \cdots, z_t]$. The other property of the z_i's is asserted in Corollary 2 to Proposition 1.1.

PROPOSITION 5. *Let* $\mathfrak{o}$ *be a Noetherian integral domain which contains a Dedekind domain* I. *Assume that the derived normal ring* $\mathfrak{o}'$ *of* $\mathfrak{o}$ *is a finite* $\mathfrak{o}$-*module. Then for all but a finite number of prime ideals* $\mathfrak{p}$ *of* I, $\mathfrak{p}\mathfrak{o}$ *has no imbedded prime divisor.*

Proof. Let $\mathfrak{P}$ be the set of prime ideals $\mathfrak{p}$ of I such that $\mathfrak{p}\mathfrak{o}$ has imbedded prime divisors. For each $\mathfrak{p} \in \mathfrak{P}$, let $S(\mathfrak{p})$ be the complement of $\mathfrak{p}$ in I. Since every element of S is a unit modulo $\mathfrak{p}$, $\mathfrak{p}\mathfrak{o}_{S(\mathfrak{p})}$ has imbedded prime divisors. Let $x_\mathfrak{p}$ be an element of $\mathfrak{p}$ such that $x_\mathfrak{p} I_\mathfrak{p} = \mathfrak{p} I_\mathfrak{p}$. Then there exists an element $a_\mathfrak{p} \in \mathfrak{o}_{S(\mathfrak{p})}$ such that $a_\mathfrak{p}/x_\mathfrak{p} \notin \mathfrak{o}_{S(\mathfrak{p})}$ and 2) $a_\mathfrak{p}/x_\mathfrak{p}$ is integral over $\mathfrak{o}_{S(\mathfrak{p})}$. Then multiplying by a suitable element of $S(\mathfrak{p})$, we may assume that $a_\mathfrak{p}/x_\mathfrak{p}$ is integral over $\mathfrak{o}$ (but $a_\mathfrak{p}/x_\mathfrak{p} \notin \mathfrak{o}$ because $a_\mathfrak{p}/x_\mathfrak{p} \notin \mathfrak{o}_{S(\mathfrak{p})}$). Since $\mathfrak{o}'$ is a finite $\mathfrak{o}$-module, there exist a finite number of $\mathfrak{p}$'s, say $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ such that all $a_\mathfrak{p}/x_\mathfrak{p}$ are in the ring $\mathfrak{o}^* = \mathfrak{o}[a_{\mathfrak{p}_1}/x_{\mathfrak{p}_1}, \cdots, a_{\mathfrak{p}_n}/x_{\mathfrak{p}_n}]$. Let x be the product of the $x_{\mathfrak{p}_i}$'s. We shall show that if $\mathfrak{p} \in \mathfrak{P}$, then $x \in \mathfrak{p}$. Indeed, if $x \notin \mathfrak{p}$, then x is in $S(\mathfrak{p})$ and $\mathfrak{o}_{S(\mathfrak{p})}$ contains $\mathfrak{o}^*$ and therefore also $a_\mathfrak{p}/x_\mathfrak{p}$, which is a contradiction. Thus $\mathfrak{P}$ is a finite set.

Remark. From the above proof, we see that if $\mathfrak{o}$ is a normal ring, then for every prime ideal $\mathfrak{p}$ of I, $\mathfrak{p}\mathfrak{o}$ has no imbedded prime divisor.

PROPOSITION 6. *Let* $\mathfrak{o}$ *and* I *be the same as in Proposition* 5. *If* d *is an element of* $\mathfrak{o}$ *which is different from zero, then for all but a finite number of prime ideals* $\mathfrak{p}$ *of* I, d *is not a zero-divisor modulo* $\mathfrak{p}\mathfrak{o}$.

Proof. Since there exist only a finite number of prime ideals $\mathfrak{p}$ of I such that $\mathfrak{p}\mathfrak{o}$ has imbedded prime divisors by Proposition 5, we may omit such prime ideals from consideration. Then d being a zero-divisor modulo $\mathfrak{p}\mathfrak{o}$ implies that d is in a minimal prime divisor of $\mathfrak{p}\mathfrak{o}$. Let S be the complement of $\mathfrak{p}$ in I. Then every prime divisor of $\mathfrak{p}\mathfrak{o}$ does not meet S and every (minimal) prime divisor of $\mathfrak{p}\mathfrak{o}_S$ is of rank 1 (because $\mathfrak{p}\mathfrak{o}_S$ is principal). Therefore, every prime divisor of $\mathfrak{p}\mathfrak{o}$ is of rank 1. Therefore, a prime divisor $\mathfrak{q}$ of $\mathfrak{p}\mathfrak{o}$ contains d if and only if $\mathfrak{q}$ is a minimal prime divisor of $d\mathfrak{o}$. Consequently, d is a zero-divisor modulo $\mathfrak{p}\mathfrak{o}$ only when $\mathfrak{p}$ is the intersection of a minimal prime divisor $\mathfrak{q}$ of $d\mathfrak{o}$ with I (except for $\mathfrak{p}$'s such that $\mathfrak{p}\mathfrak{o}$ has imbedded prime divisors). Thus we see our assertion.

THEOREM 5. *Let* $\mathfrak{o}$ *be an affine ring over a ground ring* I. *If* $\mathfrak{o}$ *is separably generated over* I, *then for all but a finite number of prime ideals* $\mathfrak{p}$ *of* I, $\mathfrak{p}\mathfrak{o}$ *is a semi-prime ideal and* $\mathfrak{o}/\mathfrak{p}'$ *is separably generated over* $I/\mathfrak{p}$ *for every prime divisor* $\mathfrak{p}'$ *of* $\mathfrak{p}\mathfrak{o}$.

Proof. We take elements $a, z_1, \cdots, z_t$ as in Theorem 4 and let L be the field of quotients of $\mathfrak{o}$. Since only a finite number of prime ideals of I contain a and a is unit modulo the remaining primes, we may consider $\mathfrak{o}[1/a]$ and $I[1/a]$ instead of $\mathfrak{o}$ and I respectively. Thus we may assume that $\mathfrak{o}$ is integral over $I[z_1, \cdots, z_t]$. Let b be an element of $\mathfrak{o}$ such that $I[z_1, \cdots, z_t, b]$ is an affine ring of L and let d be the discriminant of the irreducible monic polynomial over $I[z_1, \cdots, z_t]$ which has b as a root. Since the derived normal ring of $\mathfrak{o}$ is a finite $\mathfrak{o}$-module (because b is separable), there exist only a finite number of prime ideals $\mathfrak{p}$ of I such that d is a zero-divisor modulo $\mathfrak{p}\mathfrak{o}$ by Proposition 6 and we may omit such prime ideals from consideration. Then b modulo $\mathfrak{p}\mathfrak{o}$ ($\mathfrak{p}$ being a prime ideal of I) is separable over $I[z_1, \cdots, z_t]/\mathfrak{p}I[z_1, \cdots, z_t]$ and $\mathfrak{p}I[z_1, \cdots, z_t]$ is a semi-prime ideal. Since $\mathfrak{o}$ is contained in $I[z_1, \cdots, z_t, b, 1/d]$, and since d is not a zero-divisor modulo $\mathfrak{p}\mathfrak{o}$, we see that $\mathfrak{p}\mathfrak{o}$ is also a semi-prime ideal and that if $\mathfrak{p}'$ is a prime divisor of $\mathfrak{p}\mathfrak{o}$, then $\mathfrak{o}/\mathfrak{p}'$ is separably generated over $I/\mathfrak{p}$.

We say that a polynomial (in several indeterminates) with coefficients in an integral domain I is *absolutely irreducible* if it is irreducible even when it is regarded as a polynomial over the integral closure of I in the algebraic closure of the field of quotients of I.

PROPOSITION 7. *Let f be an absolutely irreducible polynomial in indeterminates $x_1, \cdots, x_n$ over a Noetherian integral domain I. Then for all but a finite number of prime ideals $\mathfrak{p}$ of rank 1 in I, the polynomial $f' = (f \text{ modulo } \mathfrak{p})$ is also absolutely irreducible over $I/\mathfrak{p}$.*

Proof.[4] Let d be the degree of f and e an arbitrary natural number less than d. Let $\{R_1, \cdots, R_r\}$, $\{S_1, \cdots, S_s\}$, $\{T_1, \cdots, T_t\}$ be the set of all monomials in $x_1, \cdots, x_n$ whose degrees are not greater than d, e, $d-e$ respectively, and let $y_1, \cdots, y_s$, $z_1, \cdots, z_t$ be indeterminates. Set $G = \sum y_i S_i$, $H = \sum z_j T_j$ and $F = GH$. Further we express F in the form $F = \sum w_i R_i$ or $\sum w_i' R_i$, w_i and w_i' being polynomials in $y_1, \cdots, y_s$, $z_1, \cdots, z_t$ with coefficients in the prime integral domain of I or of $I/\mathfrak{p}$ respectively. Let $X_1, \cdots, X_r$ be indeterminates, and let σ and σ' be the homomorphisms from $I[X_1, \cdots, X_r]$ onto $I[w_1, \cdots, w_r]$ and from $(I/\mathfrak{p})[X_1, \cdots, X_r]$ onto $(I/\mathfrak{p})[w'_1, \cdots, w'_r]$ respectively such that $\sigma(X_i) = w_i$ and $\sigma'(X_i) = w'_i$. Further, let $\mathfrak{q}$ and $\mathfrak{q}'$ be the kernels of σ and σ' respectively. Then 1) $\mathfrak{q}'$ contains $\mathfrak{q}$ modulo $\mathfrak{p}$, 2) if $a_1, \cdots, a_r$ are elements of I such that $g(a_1, \cdots, a_r) = 0$ for every element $g(X_1, \cdots, X_r)$ of $\mathfrak{q}$, then $\sum a_i R_i$ has a factor of degree e in some algebraic extension of I (and conversely), and 3) if $a'_1, \cdots, a'_r$ are elements of $I/\mathfrak{p}$ such that $\sum a'_i R_i$ has a factor of degree e in some algebraic extension of $I/\mathfrak{p}$, then $g'(a'_1, \cdots, a'_r) = 0$ for every element $g'(X_1, \cdots, X_r)$ of $\mathfrak{q}'$ (and conversely). Now let $c_1, \cdots, c_r$ be elements of I such that $f = \sum c_i R_i$ and let c'_i be the residue class of c_i modulo $\mathfrak{p}$ for each i. Since f is absolutely irreducible, there exists an element $g(X_1, \cdots, X_r)$ of $\mathfrak{q}$ such that $g(c_1, \cdots, c_r) \neq 0$. Let g' be g modulo $\mathfrak{p}$. Then $g' \in \mathfrak{q}'$, and f' has a factor of degree d in an algebraic extension of $I/\mathfrak{p}$ only when $g'(c'_1, \cdots, c'_r) = 0$, i.e., $g(c_1, \cdots, c_r) \in \mathfrak{p}$. Thus we see that f' has no factor of degree e in any algebraic extension of $I/\mathfrak{p}$ for all but a finite number of $\mathfrak{p}$'s. Applying this for each $e = 1, \cdots, d-1$, we prove our proposition.

THEOREM 6. *Let $\mathfrak{o}$ be an affine ring over a ground ring I. If $\mathfrak{o}$ is a regular extension of I, then for all but a finite number of prime ideals $\mathfrak{p}$ of I, $\mathfrak{p}\mathfrak{o}$ is a prime ideal and $\mathfrak{o}/\mathfrak{p}\mathfrak{o}$ is a regular extension of $I/\mathfrak{p}$.*

Proof. As in the proof of Theorem 5, we may assume that 1) $z_1, \cdots, z_t$ $(\in \mathfrak{o})$ are algebraically independent over I, 2) $\mathfrak{o}$ is integral over $I[z_1, \cdots, z_t]$

---

[4] The writer owes the present proof to Shimura [23].

and 3) $b \in \mathfrak{o}$ is separable over $I[z_1, \cdots, z_t]$, and furthermore, that $\mathfrak{o}$ and $I[z_1, \cdots, z_t, b]$ have the same field of quotients. Let $f(X)$ be the irreducible monic polynomial over $I[z_1, \cdots, z_t]$ which has b as a root and let d be the discriminant of $f(X)$. Since $\mathfrak{o}$ is a regular extension of I, $f(x)$ is absolutely irreducible as a polynomial in $z_1, \cdots, z_t, X$ over I. Therefore f modulo $\mathfrak{p}$ is absolutely irreducible for all but a finite number of prime ideals $\mathfrak{p}$ of I by Proposition 7, that is, $I[z_1, \cdots, z_t, b]/\mathfrak{p}I[z_1, \cdots, z_t, b]$ is (an integral domain and) a regular extension of $I/\mathfrak{p}$. Since we may neglect those $\mathfrak{p}$'s such that d is a zero-divisor modulo $\mathfrak{p}\mathfrak{o}$ and since $\mathfrak{o}$ is contained in $I[z_1, \cdots, z_t, b, 1/d]$, we see that $\mathfrak{o}/\mathfrak{p}\mathfrak{o}$ is a regular extension of $I/\mathfrak{p}$.

PROPOSITION 8. *Let $\mathfrak{p}$ be a prime ideal of rank r in an affine ring $\mathfrak{o}$ over a ground ring I. If $\mathfrak{o}$ is separably generated over I, then there exists a separating transcendence base $x_1, \cdots, x_n$ of $\mathfrak{o}$ over I such that* 1) *when $\mathfrak{p} \cap I = 0$, $x_1, \cdots, x_r$ is a system of parameters of $\mathfrak{o}_{\mathfrak{p}}$ and the field of quotients of $I[x_{r+1}, \cdots, x_n]$ is a basic field of $\mathfrak{o}_{\mathfrak{p}}$;* 2) *when $\mathfrak{p} \cap I \neq 0$, $x_1, \cdots, x_{r-1}, x$ (x being a prime element of $I_{(\mathfrak{p} \cap I)}$) is a system of parameters of $\mathfrak{o}_{\mathfrak{p}}$ and $I_{(\mathfrak{p} \cap I)}(x_r, \cdots, x_n)$ is a basic ring of $\mathfrak{o}_{\mathfrak{p}}$.*

Proof. When I is of characteristic zero or when $\mathfrak{p} = 0$, our assertion is obvious and we assume that I is of characteristic $p \neq 0$ and that $\mathfrak{p} \neq 0$. We set $P = \mathfrak{o}_{\mathfrak{p}}$. Let $D_1, \cdots, D_n$ be a maximal linearly independent set of derivations of $\mathfrak{o}$ over I; since $\mathfrak{o}$ is separably generated, $n =$ transcendence degree of $\mathfrak{o}$ over I by Lemma 3.3.2 and by Proposition 2. Let $y_1, \cdots, y_n$ be elements of $\mathfrak{o}$ such that $D_i y_j \neq 0$ if and only if $i = j$; here we may assume that $y_j - 1$ is in $\mathfrak{p}$ for all j because, otherwise, we may take $1 + y_i z^p$ with $z \in \mathfrak{p}$ instead of y_i (observe that $D(1 + y_i z^p) = D(y_i z^p) = z^p D y_i$ for every derivation D of $\mathfrak{o}$). On the other hand, let $z_1, \cdots, z_n$ be elements of $\mathfrak{o}$ such that 1) when $\mathfrak{p} \cap I = 0$, $z_1, \cdots, z_r$ form a system of parameters of P and $z_{r+1}, \cdots, z_n$ modulo $\mathfrak{p}$ are algebraically independent over I; 2) when $\mathfrak{p} \cap I \neq 0, x, z_1, \cdots, z_{r-1}$ form a system of parameters of P and $z_r, \cdots, z_n$ modulo $\mathfrak{p}$ are algebraically independent over $I/(\mathfrak{p} \cap I)$ (existence follows from Theorem 1.1). Set $x_i = y_i z_i^p$. Then $D_i x_j \neq 0$ if and only if $i = j$, which shows that $x_1, \cdots, x_n$ is a separating transcendence base of $\mathfrak{o}$ over I. Since $y_j - 1 \in \mathfrak{p}$, we see that these $x_1, \cdots, x_n$ are the required elements (see the proof of Proposition 1.3).

COROLLARY. *If a spot P is separably generated over a ground ring I, then there exists a basic ring B of P such that P is separably generated over B. Therefore, if P is a normal spot which is separably generated over a* *ground ring I, then there exists a basic ring B of P such that P is a regular extension of B.*

Proof. The first assertion is immediate from Proposition 8, while the last assertion follows from the first one and from the definition of regularity (take the integral closure in P of the B given by the first assertion).

Remark. In the above corollary, if I satisfies the finiteness condition for integral extensions, then we can select B to satisfy the same condition, as is easily seen from our proof by virtue of Proposition 1. 2.

5. A lemma due to Zariski.

LEMMA 1. *Let L be a finite algebraic extension of a field K. If there exists an element a of L such that L is separable over $K(a)$, then L is a simple extension of K, that is, there exists an element c of L such that $L=K(c)$.*

Proof. Let L' be the maximal separable subfield of L over K. Then there exists an element d of L' such that $L'=K(d)$. Let b be an element of L such that $L=K(a,b)$. Then b is purely inseparable over $K(a,d)$ and separable over $K(a,d)$. Thus b is in $K(a,d)$ and $L=K(a,d)$. Since d is separable over K, $L=K(a,d)$ is a simple extension of K.

LEMMA 2. *Let L be a simple algebraic extension of a field K. Then the number of fields L' such that $K\subseteq L'\subseteq L$ is at most 2^{n-1}, where n is the degree of L over K.*

Proof. Let b be an element of L such that $L=K(b)$, and let $b=b_1, b_2,\cdots, b_n$ be the conjugates of b (if L is inseparable over K, each b_i appears just $[L:K]_i$-times). If $K\subseteq L'\subseteq L$, then there are $i_1,\cdots,i_r$ (each $i_j>1$) such that $(x-b)(x-b_{i_1})\cdots(x-b_{i_r})$ is the irreducible polynomial over L' which has b as a root. Then the field generated over K by the coefficients of this polynomial coincides with L' because $L=L'(b)$. Therefore, there exists a one-to-one correspondence between L' and a family of subsets of $2,\cdots,n$, which proves our assertion.

The following lemma is obvious.

LEMMA 3. *Assume that a function field L over a field $\mathbf{k}$ is separably generated over $\mathbf{k}$. Then for an element x of L, the following three conditions are equivalent to each other:*

1) *There exists a derivation D of L over $\mathbf{k}$ such that $Dx\neq 0$.*

2) *There exists a separating transcendence base of L over $\boldsymbol{k}$ which has x as a member.*

3) *When $\boldsymbol{k}$ is of characteristic zero, x is transcendental over $\boldsymbol{k}$; when $\boldsymbol{k}$ is of characteristic $p \neq 0$, x is not in $\boldsymbol{k}(L^p)$.*

Remark. Let L be a function field over a field $\boldsymbol{k}$ of characteristic $p \neq 0$, and let $x_1, \cdots, x_n$ be elements of L such that $L = \boldsymbol{k}(L^p)(x_1, \cdots, x_n)$ with n such that $[L : \boldsymbol{k}(L^p)] = p^n$. Then the derivations $D_1, \cdots, D_n$, such that $D_i x_j$ is 1 or 0 according as $i = j$ or $i \neq j$, form a maximal linearly independent set of derivations of L over $\boldsymbol{k}$.

Now, making use of the above lemmas, we shall prove a generalization of a lemma due to Zariski [25] by the methods of Zariski [25] and Matusaka [10]:

THEOREM 7. *Let L be a function field over a ground field $\boldsymbol{k}$.*[5] *Assume that x and y are elements of L which are algebraically independent over $\boldsymbol{k}$ and that there exists a derivation D of L over $\boldsymbol{k}$ such that $Dx \neq 0$. Let L' be the algebraic closure of $\boldsymbol{k}(x, y)$ in L. If L is a regular extension of $\boldsymbol{k}$, then L is a regular extension of $\boldsymbol{k}(x + cy)$ for all except possibly $2^{n-1} + 1$ elements c of $\boldsymbol{k}$, where $n = [L' : \boldsymbol{k}(x, y)]$.*

Proof. For every element c of $\boldsymbol{k}$, we denote by $\boldsymbol{k}_c$ the algebraic closure of $\boldsymbol{k}(x + cy)$ in L' (hence in L). Consider the following conditions for an element c of $\boldsymbol{k}$: 1) $D(x + cy) \neq 0$ and 2) there exists an element d $(\neq c)$ of $\boldsymbol{k}$ such that $\boldsymbol{k}_c(x + dy) = \boldsymbol{k}_d(x + cy)$. Since $D(x + cy) = Dx + cDy$ and since $Dx \neq 0$, there exists at most one c which does not satisfy the condition 1). On the other hand, since $x \notin \boldsymbol{k}(L'^p)$, there exists an element z of L' such that x and z form a separating transcendence base of L' over $\boldsymbol{k}$, and if w is an element of L' such that $L' = \boldsymbol{k}(x, z, w)$, then $L' = \boldsymbol{k}(x, y)(z, w)$, and w is separable over $\boldsymbol{k}(x, y, z)$ and L' is a simple extension of $\boldsymbol{k}(x, y)$ by Lemma 1. Since $\boldsymbol{k}_c(x + dy) = \boldsymbol{k}(x, y)(\boldsymbol{k}_c)$, the number of c's which do not satisfy the condition 2) is not greater than 2^{n-1} by Lemma 2. Therefore, we have only to show that if an element $c \in \boldsymbol{k}$ satisfies the conditions 1) and 2), then L is a regular extension of $\boldsymbol{k}(x + cy)$. Since $\boldsymbol{k}_d$ is a regular extension of $\boldsymbol{k}$ by Theorem 3 and since $x + cy$ is transcendental over $\boldsymbol{k}_d$, $\boldsymbol{k}_d(x + cy) = \boldsymbol{k}_c(x + dy)$ is a regular extension of $\boldsymbol{k}(x + cy)$ by Corollary 1 to Theorem 3. Since $\boldsymbol{k}_c$ is algebraic over $\boldsymbol{k}(x + cy)$, we have $\boldsymbol{k}_c = \boldsymbol{k}(x + cy)$, which shows that $\boldsymbol{k}(x + cy)$ is algebraically closed in L. Since $D(x + cy) \neq 0$, there exists a separating transcendence base of L over $\boldsymbol{k}$ which has $x+cy$ as a member, which shows that L is a regular extension of $\boldsymbol{k}(x+cy)$ and the proof is completed.

---

[5] By the definition of regularity, the assumption that k is a field is not essential.

COROLLARY 1. *With the same L, $\boldsymbol{k}$, x and y as above, if u is transcendental over L, then $L(u)$ is a regular extension of $\boldsymbol{k}(u)(x+uy)$.*

Proof. Let $u_1,\cdots,u_N$ ($N>2^{n-1}+1$ with the same n as above) be algebraically independent elements over L. Let L' be the same as above. $L'(u_1,\cdots,u_N)$ is the algebraic closure of $\boldsymbol{k}(u_1,\cdots,u_N,x,y)$ in $L(u_1,\cdots,u_N)$ and $[L'(u_1,\cdots,u_N):\boldsymbol{k}(u_1,\cdots,u_N,x,y)]=n$. Therefore, there exists one i such that $L(u_1,\cdots,u_N)$ is a regular extension of $\boldsymbol{k}(u_i)(x+u_iy)$. It follows that $L(u_i)$ is a regular extension of $\boldsymbol{k}(u_i)(x+u_iy)$ because $u_1,\cdots,u_{i-1},u_{i+1},\cdots,u_N$ are algebraically independent over $\boldsymbol{k}(u_i)(x+u_iy)$. Since u_i is transcendental over L, we may replace u_i by u, which proves our assertion.

COROLLARY 2. *Assume that an integral domain $\mathfrak{o}$ is generated by $x_1,\cdots,x_N$ over a subring I. If $\mathfrak{o}$ is a regular extension of I, if I contains infinitely many elements and if the transcendence degree of $\mathfrak{o}$ over I is greater than 1, then there exists a linear combination $\sum a_ix_i$ ($a_i\in I$) such that $\mathfrak{o}$ is a regular extension of $I[\sum a_ix_i]$.*

6. Tensor products of normal rings.

LEMMA 1. *Let $\mathfrak{o}$ be a normal ring which contains a field $\boldsymbol{k}$. If a field K is separably generated over $\boldsymbol{k}$ and if $K\otimes_k\mathfrak{o}$ is an integral domain, then $K\otimes_k\mathfrak{o}$ is a normal ring.* (Y. Nakai)

Proof. We may assume that K is finitely generated over $\boldsymbol{k}$. Let $x_1,\cdots,x_n$ be a separating transcendence base of K over $\boldsymbol{k}$ and set $\mathfrak{s}=\mathfrak{o}[x_1,\cdots,x_n]$, $\boldsymbol{k}'=\boldsymbol{k}(x_1,\cdots,x_n)$ (with regard to the fact that K and $\mathfrak{o}$ are subrings of $K\otimes\mathfrak{o}$). Since $x_1,\cdots,x_n$ are algebraically independent over $\mathfrak{o}$ and since $\mathfrak{o}$ is a normal ring, we see that $\mathfrak{s}$ is a normal ring. Since $\boldsymbol{k}'[\mathfrak{o}]$ is a ring of quotients of $\mathfrak{s}$, $\boldsymbol{k}'[\mathfrak{o}]$ is a normal ring. Now since every element of K is a root of a monic polynomial over $\boldsymbol{k}'$ (hence over $\boldsymbol{k}'[\mathfrak{o}]$) whose discriminant is a unit in $\boldsymbol{k}'$ (hence in $\boldsymbol{k}'[\mathfrak{o}]$), we see that $K[\mathfrak{o}]$ ($=K\otimes\mathfrak{o}$) is a normal ring.

THEOREM 8. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be normal rings which contain a field $\boldsymbol{k}$. If $\mathfrak{o}$ and $\mathfrak{o}'$ are separably generated over $\boldsymbol{k}$ and if $\mathfrak{o}\otimes_k\mathfrak{o}'$ is an integral domain, then $\mathfrak{o}\otimes_k\mathfrak{o}'$ is a normal ring.* (Y. Nakai)

Proof. Let L and L' be the fields of quotients of $\mathfrak{o}$ and $\mathfrak{o}'$ respectively. By Lemma 1, $L \otimes \mathfrak{o}'$ and $\mathfrak{o} \otimes L'$ are normal rings. Therefore, we have only to show that $(L \otimes \mathfrak{o}') \cap (\mathfrak{o} \otimes L') = \mathfrak{o} \otimes \mathfrak{o}'$. Let $\{u_\lambda\}$ and $\{u'_{\lambda'}\}$ be linearly independent bases of $\mathfrak{o}$ and $\mathfrak{o}'$ over $\boldsymbol{k}$, and let $\{v_\mu\}$ and $\{v'_{\mu'}\}$ be linearly independent bases of L and L' over $\boldsymbol{k}$ which contain $\{u_\lambda\}$ and $\{u'_{\lambda'}\}$ respectively. Then every element b of $L \otimes L'$ is expressed uniquely in the form $\sum v_\mu v'_{\mu'} a_{\mu\mu'}$ $(a_{\mu\mu'} \in \boldsymbol{k})$. If b is in $L \otimes \mathfrak{o}'$, then in this expression $v'_{\mu'}$ is in $\{u'_{\lambda'}\}$ for all μ' such that $a_{\mu\mu'} \neq 0$; if b is in $\mathfrak{o} \otimes L'$, then v_μ is in $\{u_\lambda\}$ for all μ such that $a_{\mu\mu'} \neq 0$. Therefore, if b is in $(L \otimes \mathfrak{o}') \cap (\mathfrak{o} \otimes L')$, then the expression must be of the form $\sum u_\lambda u'_{\lambda'} a_{\lambda\lambda'}$ $(a_{\lambda\lambda'} \in \boldsymbol{k})$, that is $b \in \mathfrak{o} \otimes \mathfrak{o}'$. Thus we see that $(L \otimes \mathfrak{o}') \cap (\mathfrak{o} \otimes L') = \mathfrak{o} \otimes \mathfrak{o}'$ and the proof is completed.

The analogue of Theorem 8 does not hold in general for tensor products over a ring which is not a field, even if the ring is the case over a ground place. Though we shall discuss below under what condition such an extended result does hold, we shall first give a counter example:

Example. Let I be the ring of rational integers and let x and y be algebraically independent elements over I. Set $I^* = I_{2I}$ and $I' = I^*(x, y)$. Then I' is a discrete valuation ring with a prime element 2 and is a ground place. Let z, z', w, w' be algebraically independent elements over I' and set $\mathfrak{o} = I'[z, w, \sqrt{x + 2z}, \sqrt{y + 2w}]$, $\mathfrak{o}' = I'[z', w', \sqrt{x + 2z'}, \sqrt{y + 2w'}]$. Then $\mathfrak{o}$ and $\mathfrak{o}'$ are regular extensions of I', and $2\mathfrak{o}$ and $2\mathfrak{o}'$ are prime ideals. Set $P = \mathfrak{o}_{2\mathfrak{o}}$, $P' = \mathfrak{o}'_{2\mathfrak{o}'}$. Then P and P' are the valuation rings, hence they are normal spots over I' (and they are regular extensions of I'). Since $(P \otimes_{I'} P')/(2) = (P/2P) \otimes_{I'/2I'} (P'/2P')$, we see that there exists only one minimal prime divisor $\mathfrak{p}$ of $2(P \otimes P')$ and that $\mathfrak{p}(P \otimes P')_{\mathfrak{p}}/(2)$ is not principal. Therefore $\mathfrak{p}(P \otimes P')_{\mathfrak{p}}$ is not principal. Since $\mathfrak{p}$ is of rank 1, it follows that $(P \otimes P')_{\mathfrak{p}}$ is not normal and $P \otimes P'$ is also not normal.

PROPOSITION 9. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be normal rings which contain a discrete valuation ring I with a prime element x. Assume that $\mathfrak{o}^* = \mathfrak{o} \otimes_I \mathfrak{o}'$ is a Noetherian integral domain and that both $\mathfrak{o}$ and $\mathfrak{o}'$ are separably generated over I. Then $\mathfrak{o}^*$ is a normal ring if and only if $\mathfrak{o}^*_{\mathfrak{p}^*}$ is a normal ring for every prime divisor $\mathfrak{p}^*$ of $x\mathfrak{o}^*$.*

Proof. Let $\boldsymbol{k}$ be the field of quotients of I. Then $\boldsymbol{k} = I[1/x]$ and we have $\mathfrak{o}^*[1/x] = \mathfrak{o}[1/x] \otimes \mathfrak{o}'[1/x]$ by Theorem 1. Therefore $\mathfrak{o}^*[1/x]$ is a normal ring by Theorem 8. Now we prove our assertion easily (see [16, § 9]).

COROLLARY. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be normal affine rings or spots over the same ground ring I. Assume that I is a valuation ring with a prime element x.*

If the following four conditions are satisfied, then $\mathfrak{o}\otimes_I\mathfrak{o}'$ *is a normal ring.*

1) $\mathfrak{o}$ *and* $\mathfrak{o}'$ *are separably generated over* I.

2) $x\mathfrak{o}$ *and* $x\mathfrak{o}'$ *are semi-prime ideals.*

3) $\mathfrak{o}\otimes\mathfrak{o}'$ *is an integral domain.*

4) *If* $\mathfrak{p}$ *and* $\mathfrak{p}'$ *are prime divisors of* $x\mathfrak{o}$ *and* $x\mathfrak{o}'$ *respectively, then* $(\mathfrak{o}/\mathfrak{p})\otimes_{I/xI}(\mathfrak{o}'/\mathfrak{p}')$ *has no nilpotent elements.*

Proof. By our assumption, $x(\mathfrak{o}\otimes\mathfrak{o}')$ is a semi-prime ideal and we see the assertion by Proposition 9.

Remark 1. Condition 4) is satisfied if one of $\mathfrak{o}/\mathfrak{p}$ and $\mathfrak{o}'/\mathfrak{p}'$ is separably generated over I/xI by Theorem 1.

Remark 2. Since the intersection of normal rings is again a normal ring, we can apply Proposition 9 and its corollary to tensor products over a Dedekind domain by virtue of Theorem 1.

Chapter 4. Preliminary Results from the Theory of Regular Local Rings.

1. Ring extensions of regular local rings.

PROPOSITION 1. *Let* $\mathfrak{o}$ *be a local integral domain with maximal ideal* $\mathfrak{m}$ *and let* a *be an element of an integral extension of* $\mathfrak{o}$. *Assume that* 1) a *is not in the field of quotients of* $\mathfrak{o}$, 2) *the characteristic* p *of* $\mathfrak{o}$ *is different from zero and* 3) $a^p\in\mathfrak{o}$. *Then* $\mathfrak{o}[a]$ *is a local ring. Furthermore, the dimension of the vector space* $\mathfrak{m}'/\mathfrak{m}'^2$ *over* $\mathfrak{o}'/\mathfrak{m}'$ *is not less than that of* $\mathfrak{m}/\mathfrak{m}^2$ *over* $\mathfrak{o}/\mathfrak{m}$ ($\mathfrak{m}'$ *being the maximal ideal of* $\mathfrak{o}'$); *they coincide with each other if and only if either the irreducible polynomial* X^p-a^p *over* $\mathfrak{o}$ *is irreducible modulo* $\mathfrak{m}$, *or there exists an element* $b\in\mathfrak{o}$ *such that* $(a-b)^p\in\mathfrak{m},\notin\mathfrak{m}^2$.

Proof. Since a is purely inseparable over $\mathfrak{o}$, $\mathfrak{o}[a]$ is a local ring. Let $x_1,\cdots,x_r$ be a minimal base of $\mathfrak{m}$.[6]

1) When X^p-a^p is irreducible modulo $\mathfrak{m}$, it is easy to see that $\mathfrak{m}'$ is generated by $\mathfrak{m}$. Furthermore, $x_1,\cdots,x_r$ is a minimal base of $\mathfrak{m}'$. For, otherwise, there exists an element x of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$ such that $x\in\mathfrak{m}'^2=\mathfrak{m}^2\mathfrak{o}[a]$, which is impossible because $1,a,\cdots,a^{p-1}$ are linearly independent over $\mathfrak{o}$. Thus the case is settled.

---

[6] We call a base of an ideal is minimal if any proper subset of the base cannot generate the ideal. When $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{m}$, a subset of an ideal $\mathfrak{a}$ of $\mathfrak{o}$ generates $\mathfrak{a}$ if and only if their residue classes modulo $\mathfrak{m}\mathfrak{a}$ generates $\mathfrak{a}/\mathfrak{m}\mathfrak{a}$ over $\mathfrak{o}/\mathfrak{m}$. Therefore r is equal to the dimension of $\mathfrak{m}/\mathfrak{m}^2$ in the present case.

2) Assume that $X^p - a^p$ is reducible modulo $\mathfrak{m}$. Then there exists an element $b \in \mathfrak{o}$ such that $a^p - b^p \in \mathfrak{m}$. Therefore, considering $a - b$ instead of a, we may assume that $b = 0$, that is, $a \in \mathfrak{m}'$. Assume that an element $x \in \mathfrak{m}$ which is not in $\mathfrak{m}^2$ is in $\mathfrak{m}'^2$. Then, since $\mathfrak{m}' = \mathfrak{m}\mathfrak{o}[a] + a\mathfrak{o}[a] = \mathfrak{m} + a\mathfrak{o}[a]$, there is a relation of the form:

$$x = \sum c_{ij}x_ix_j + (\sum d_jx_j)a + (\textstyle\sum_0^{p-1} e_ia^i)a^2 \qquad (c_{ij}, d_j, e_i \in \mathfrak{o}).$$

Since $1, a, \cdots, a^{p-1}$ are linearly independent over $\mathfrak{o}$, we have

$$x = \sum c_{ij}x_ix_j + e_{p-2}a^p.$$

This shows that the residue class of x modulo $\mathfrak{m}^2$ is of the form unit × (a^p modulo $\mathfrak{m}^2$). Therefore, the dimension of $\mathfrak{m}'/\mathfrak{m}'^2$ is either r or $r+1$ according as $a^p \notin \mathfrak{m}^2$ or $a^p \in \mathfrak{m}^2$. Thus the proof is completed.

COROLLARY 1. *If furthermore* $\mathfrak{o}[a]$ *is a regular local ring, then so is* $\mathfrak{o}$.

COROLLARY 2. *Besides the assumptions in Proposition* 1, *we assume that* $\mathfrak{o}$ *is a regular local ring. Then* $\mathfrak{o}[a]$ *is regular if and only if either* $X^p - a^p$ *is irreducible modulo* $\mathfrak{m}$, *or there exists an element* b *of* $\mathfrak{o}$ *such that* $(a - b)^p \in \mathfrak{m}, \notin \mathfrak{m}^2$.

PROPOSITION 2. *Let* $\mathfrak{o}$ *be a normal local ring and let* a *be a root of an irreducible monic polynomial* $f(x)$ *over* $\mathfrak{o}$. *Let* $\mathfrak{p}$ *be a maximal ideal of* $\mathfrak{o}[a]$, *and set* $\mathfrak{o}' = \mathfrak{o}[a]_{\mathfrak{p}}$, $\mathfrak{m}' = \mathfrak{p}\mathfrak{o}'$. *If the discriminant* d *of* $f(x)$ *is a unit in* $\mathfrak{o}$, *then* 1) $\mathfrak{m}' = \mathfrak{m}\mathfrak{o}'$ *and* 2) $\mathfrak{o}'$ *is a normal ring.*

Proof. Since d is a unit in $\mathfrak{o}$, we have that $\mathfrak{o}[a]$ is a normal ring, and 2) follows immediately. Let $g(x)$ be a monic polynomial over $\mathfrak{o}$ such that i) $g(x)$ modulo $\mathfrak{m}$ is irreducible over $\mathfrak{o}/\mathfrak{m}$ and ii) a modulo $\mathfrak{p}$ is a root of $g(x)$ modulo $\mathfrak{m}$. Set $b = g(a)$. Then $b \in \mathfrak{p}$. Set $\mathfrak{p}'' = \mathfrak{m}\mathfrak{o}[b] + b\mathfrak{o}[b]$, which is a maximal ideal of $\mathfrak{o}[b]$ and $\mathfrak{p}'' = \mathfrak{p} \cap \mathfrak{o}[b]$. Since $g(x)$ modulo $\mathfrak{m}$ is irreducible over $\mathfrak{o}/\mathfrak{m} = \mathfrak{o}[b]/\mathfrak{p}''$, $\mathfrak{p} = \mathfrak{p}''\mathfrak{o}[a]$. It follows, in particular, that $\mathfrak{p}$ is the unique maximal ideal of $\mathfrak{o}[a]$ containing b. Let $h(x)$ be a monic polynomial over $\mathfrak{o}$ such that i) $f(x) - g(x)h(x) \in \mathfrak{m}[x]$ and ii) every irreducible factor of $h(x)$ is irreducible modulo $\mathfrak{m}$. Then applying the same observation to each irreducible factor of $h(x)$, we see that $c = h(a)$ is not in $\mathfrak{p}$ (because d is a unit and $g(x)$, $h(x)$ have no common factor modulo $\mathfrak{m}$). Since $g(a) = b$, $bc \in \mathfrak{m}\mathfrak{o}[a]$ and $b \in \mathfrak{m}\mathfrak{o}'$, which shows that $\mathfrak{m}' = \mathfrak{m}\mathfrak{o}'$ (because $\mathfrak{p} = \mathfrak{p}''\mathfrak{o}[a]$).

COROLLARY. *If furthermore* $\mathfrak{o}$ *is a regular local ring, then* $\mathfrak{o}'$ *is also a regular local ring.*

PROPOSITION 3. *Let* $\mathfrak{o}$ *be an integral domain and let* $x_1, \cdots, x_n$ *be algebraically independent elements over* $\mathfrak{o}$. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{o}' = \mathfrak{o}[x_1, \cdots, x_n]$. *If* $\mathfrak{o}_{(\mathfrak{p} \cap \mathfrak{o})}$ *is a regular local ring, then so is* $\mathfrak{o}'_{\mathfrak{p}}$.

Proof. By Corollary 5 to Proposition 1.1, $\mathfrak{o}'_{\mathfrak{p}}/(\mathfrak{p} \cap \mathfrak{o})\mathfrak{o}'_{\mathfrak{p}}$ is a regular local ring, from which the assertion follows immediately.

LEMMA 1. *Let* x *be a transcendental element over a local ring* $\mathfrak{o}$. *Then a minimal base of the maximal ideal* $\mathfrak{m}$ *of* $\mathfrak{o}$ *is also a minimal base of* $\mathfrak{m}\mathfrak{o}(x)$. *Therefore,* $\mathfrak{o}$ *is regular if and only if* $\mathfrak{o}(x)$ *is.*

The proof is easy.

COROLLARY. *The converse of Proposition* 3 *holds.*

Proof. From the regularity of $\mathfrak{o}'_{\mathfrak{p}}$ and $\mathfrak{o}'_{\mathfrak{p}}/(\mathfrak{p} \cap \mathfrak{o})\mathfrak{o}'_{\mathfrak{p}}$, it follows that $(\mathfrak{p} \cap \mathfrak{o})\mathfrak{o}'_{\mathfrak{p}}$ is generated by a subset of a regular system of parameters of $\mathfrak{o}'_{\mathfrak{p}}$ (Lemma 0.12) and $\mathfrak{o}'_{(\mathfrak{p} \cap \mathfrak{o})\mathfrak{o}'} = \mathfrak{o}(x_1, \cdots, x_n)$ is regular, from which it follows that $\mathfrak{o}_{(\mathfrak{p} \cap \mathfrak{o})}$ is regular.

LEMMA 2. *Let* $\mathfrak{o}$ *be a regular local ring with maximal ideal* $\mathfrak{m}$. *If a monic polynomial* $f(x)$ *over* $\mathfrak{o}$ *is irreducible modulo* $\mathfrak{m}$, *then the ring* $\mathfrak{o}' = \mathfrak{o}[x]/f(x)\mathfrak{o}[x]$ *is a regular local ring with maximal ideal* $\mathfrak{m}\mathfrak{o}'$. *Further,* $\mathfrak{m}^n\mathfrak{o}' \cap \mathfrak{o} = \mathfrak{m}^n$ for every $n = 1, 2, \cdots$.

Proof. Since $f(x)$ itself is also irreducible, the assertion is proved easily.

Remark. By the same way as above, we see that Lemma 2 can be generalized as follows: Let $\mathfrak{o}$ be a normal local ring with maximal ideal $\mathfrak{m}$. If a monic polynomial $f(x)$ over $\mathfrak{o}$ is irreducible modulo $\mathfrak{m}$, then the ring $\mathfrak{o}' = \mathfrak{o}[x]/f(x)\mathfrak{o}[x]$ is a local ring with maximal ideal $\mathfrak{m}\mathfrak{o}'$ and $\mathfrak{m}^n\mathfrak{o} \cap \mathfrak{o} = \mathfrak{m}^n$. Therefore, if $\mathfrak{o}'$ is regular, then $\mathfrak{o}$ is also a regular local ring.

2. Quadratic transforms of local integral domains. Let $\mathfrak{o}$ be a local integral domain with maximal ideal $\mathfrak{m}$ and let $x_1, \cdots, x_n$ be a base of $\mathfrak{m}$. Further, let $\mathfrak{v}$ be a valuation ring which dominates $\mathfrak{o}$ and let $\mathfrak{n}$ be the maximal ideal of $\mathfrak{v}$. Let v be a valuation whose valuation ring is $\mathfrak{v}$. We may assume that $v(x_1) \leqq v(x_j)$ for every j. Set $\mathfrak{o}' = \mathfrak{o}[x_2/x_1, \cdots, x_n/x_1]$, $\mathfrak{m}' = \mathfrak{n} \cap \mathfrak{o}'$ (observe that $\mathfrak{o}'$ is a subring of $\mathfrak{v}$), $\mathfrak{o}'' = \mathfrak{o}'_{\mathfrak{m}'}$ and $\mathfrak{m}'' = \mathfrak{m}'\mathfrak{o}''$. Then

PROPOSITION 4. 1) $\mathfrak{o}''$ *is a local integral domain*; 2) $\mathfrak{o}''$ *is determined by* $\mathfrak{v}$ *above, that is,* $\mathfrak{o}''$ *is independent of the choice of the base* $x_1, \cdots, x_n$

of $\mathfrak{m}$; 3) *if* $\mathfrak{p}$ *is a prime ideal of* $\mathfrak{o}$ *which does not contain* x_1 *and if there exists a prime ideal* $\mathfrak{p}''$ *of* $\mathfrak{o}''$ *such that* $\mathfrak{o}_{\mathfrak{p}}$ *is dominated by* $\mathfrak{o}''_{\mathfrak{p}''}$, *then* $\mathfrak{o}_{\mathfrak{p}} = \mathfrak{o}''_{\mathfrak{p}''}$; *and* 4) *if* $\mathfrak{o}$ *is a regular local ring, then* $\mathfrak{o}''$ *is also a regular local ring.*

This $\mathfrak{o}''$ is called the *quadratic transform* of $\mathfrak{o}$ with respect to the valuation ring $\mathfrak{v}$.

Proof. (1) Since $\mathfrak{o}$ is a Noetherian ring and since $\mathfrak{o}'$ is finitely generated over $\mathfrak{o}$, $\mathfrak{o}'$ is Noetherian and $\mathfrak{o}''$ is a local integral domain.

(2) Let $y_1, \cdots, y_m$ be another base of $\mathfrak{m}$. In order to prove 2), we may assume that $x_j = y_j$ for $j \leqq n$. First set $\mathfrak{o}^* = \mathfrak{o}[y_2/y_1, \cdots, y_m/y_1]$. Then $\mathfrak{o}' \subseteq \mathfrak{o}^*$. Since y_i is a linear combination of x_j's with coefficients in $\mathfrak{o}$, we have $\mathfrak{o}' = \mathfrak{o}^*$ and $\mathfrak{o}'' = \mathfrak{o}^*_{(\mathfrak{n} \cap \mathfrak{o}^*)}$. Assume that $v(y_i) = v(y_1)$ $(= v(x_1))$. Set $\mathfrak{o}^{**} = \mathfrak{o}[y_1/y_i, \cdots, y_m/y_i]$. Then $y\ /y_i$ is a unit in $\mathfrak{v}$ and $y\ /y_i$ is not in $\mathfrak{m}^{**} = \mathfrak{n} \cap \mathfrak{o}^{**}$. Therefore $\mathfrak{o}^{**}{}_{\mathfrak{m}^{**}}$ contains y_1/y_i as a unit, hence $\mathfrak{o}^{**}{}_{\mathfrak{m}^{**}}$ contains $y_2/y_1, \cdots, y_m/y_1$. Therefore $\mathfrak{o}^*{}_{\mathfrak{m}^*} \subseteq \mathfrak{o}^{**}{}_{\mathfrak{m}^{**}}$. By the same reason, we have the converse inclusion, and $\mathfrak{o}'' = \mathfrak{o}_{\mathfrak{m}^*} = \mathfrak{o}^{**}{}_{\mathfrak{m}^{**}}$.

(3) Since $x_1 \notin \mathfrak{p}$, $\mathfrak{o}'$ is a subring of $\mathfrak{o}_{\mathfrak{p}}$ and 3) is easy.

(4) By 2), we may assume that $x_1, \cdots, x_n$ is a regular system of parameters of $\mathfrak{o}$. $\mathfrak{m}$ is contained in $x_1\mathfrak{o}'$, and $\mathfrak{o}'/x\mathfrak{o}'$ is generated by the residue classes of $x_2/x_1, \cdots, x_n/x_1$ over the residue class field of $\mathfrak{o}$; they are obviously algebraically independent over $\mathfrak{o}/\mathfrak{m}$. Therefore, $\mathfrak{o}''/x_1\mathfrak{o}''$ is a regular local ring by Corollary 5 to Proposition 1.1, which shows that $\mathfrak{o}''$ is also a regular local ring.

Remark. Observe that if $v(x_1) < v(x_j)$ for every $j > 1$, then the maximal ideal of $\mathfrak{o}''$ is generated by x_1, $x_2/x_1, \cdots, x_n/x_1$.

3. Results due to Serre [22]. If M is module over a ring $\mathfrak{o}$, the projective dimension of M in the sense of Cartan-Eilenberg [2] is called the *homological dimension* of M (according to Serre [22]), which will be denoted by $\mathrm{dh}_{\mathfrak{o}} M$ or by $\mathrm{dh}\, M$. A series $a_1, \cdots, a_r$ of elements of the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$ is called an *M-series* if for every $i \leqq r$ the element a_i is not a zero-divisor in the module $M/(\sum_1^{i-1} a_j M)$. The number r is called the length of the series.

Proposition 5. *If* M *is a finite module over a regular local ring* $\mathfrak{o}$ *of rank* n, *then every maximal M-series is of length* $n - \mathrm{dh}\, M$. (Auslander-Buchsbaum-Serre)

For the proof, see Serre [22].

COROLLARY. *If* $\mathfrak{a}$ *is an ideal of* $\mathfrak{o}$ *and if* $n \geqq 1$, *then* $\mathrm{dh}\,\mathfrak{a} \leqq n-1$; *if* $\mathfrak{p}$ *is a prime ideal of* $\mathfrak{o}$ *different from* $\mathfrak{m}$ *and if* $n \geqq 2$, *then* $\mathrm{dh}\,\mathfrak{p} \leqq n-2$.

THEOREM 1. *If* $\mathfrak{p}$ *is a prime ideal of a regular local ring* $\mathfrak{o}$, *then* $\mathfrak{o}_{\mathfrak{p}}$ *is a regular local ring.* (Serre [22])

For the proof, see Serre [22]; the base of his proof is the following

PROPOSITION 6. *A local ring* $\mathfrak{o}$ *is regular if and only if there exists an integer* m *such that* $\mathrm{dh}\,M \leqq m$ *for every* $\mathfrak{o}$*-module* M (*that is, global homological dimension of* $\mathfrak{o}$ *is finite*). (Serre [22])

For the proof, see Serre [22].

In the latter parts of our papers, we shall need only Theorem 1 in the case where $\mathfrak{o}$ is a spot of the restricted case, among results stated here. Therefore, we shall give another proof for this case in Appendix 1. (A proof for this case is also given by Nagata [18].)

4. Unramifiedness of regular local rings. Let $\mathfrak{r}$ be a regular local ring with a semi-ground ring I. We say that $\mathfrak{r}$ is *unramified* with respect to I if either $\mathfrak{r}$ contains the field of quotients of I, or a prime element of $I_{(\mathfrak{m} \cap I)}$ is not in $\mathfrak{m}^2$, where $\mathfrak{m}$ denotes the maximal ideal of $\mathfrak{r}$ (that is, a prime element of $I_{(\mathfrak{m} \cap I)}$ can be selected to be a member of a regular system of parameters of $\mathfrak{r}$). If furthermore the residue class field of $\mathfrak{r}$ is separably generated over that of $I_{(\mathfrak{m} \cap I)}$, then we say that $\mathfrak{r}$ is *tamely unramified* (with respect to I).

A spot P over a ground ring I is called a simple spot if it is a regular local ring. It is called an *unramified simple spot* (over I) if it is unramified with respect to I; it is called a *tamely unramified* simple spot if it is tamely unramified. It is called *ramified* (over I) if it is not unramified.

Remark. Since an "unramified regular local ring" is a regular local ring which contains a field or in which p is not in the square of the maximal ideal of the ring (p being the characteristic of the residue class field of the ring), we must distinguish between unramified simple spots and simple spots which are unramified regular local rings.

PROPOSITION 7. *If* P *is a tamely unramified regular local ring with respect to a semi-ground ring* I, *then the completion* P^* *of* P *contains a complete discrete valuation ring* I^* (*which may be a field*) *such that* 1) I *is a subring of* I^* *and* 2) P^* *is a formal power series ring over* I^*.

The proof is easy because P^* is a Henselian ring (Lemma 0.13).

THEOREM 2. *Let* $\mathfrak{p}$ *be a prime ideal of a regular local ring* $\mathfrak{r}$. *If* $\mathfrak{r}$ *is unramified with respect to a semi-ground ring* I, *then* $\mathfrak{r}_{\mathfrak{p}}$ *is also unramified with respect to* I.

Proof.[7] Set $\mathfrak{q} = \mathfrak{p} \cap I$. If $\mathfrak{q} = 0$, then $\mathfrak{r}_{\mathfrak{p}}$ contains the field of quotients k of I and $\mathfrak{r}_{\mathfrak{p}}$ is unramified with respect to I. Assume that $\mathfrak{q} \neq 0$. Let x be a prime element of $I_{\mathfrak{q}}$. Since $\mathfrak{r}$ is unramified with respect to I, $\mathfrak{r}/x\mathfrak{r}$ is a regular local ring. Therefore, by Theorem 1, $(\mathfrak{r}/x\mathfrak{r})_{(\mathfrak{p}/x\mathfrak{r})} = \mathfrak{r}_{\mathfrak{p}}/x\mathfrak{r}_{\mathfrak{p}}$ is a regular local ring, which proves that $\mathfrak{r}_{\mathfrak{p}}$ is unramified with respect to I.

More generally, we can prove the following assertion, making use of the notion of quadratic transformation (cf. § 2) or some results in Nagata [18]:

Let $\mathfrak{o}$ *be a regular local ring with maximal ideal* $\mathfrak{m}$ *and let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{o}$. *If an element* f *of* $\mathfrak{p}$ *is not in* $\mathfrak{m}^n$, *then* f *is not in* $\mathfrak{p}^n\mathfrak{o}_{\mathfrak{p}}$.

We shall here only sketch the proofs. Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$ and let $\mathfrak{p}^*$ be a prime divisor of $\mathfrak{p}\mathfrak{o}^*$. Then $\mathfrak{p}^* \cap \mathfrak{o} = \mathfrak{p}$ by the corollary to Lemma 0.4, $\mathfrak{p}^{*n}\mathfrak{o}^*_{\mathfrak{p}^*}$ contains $\mathfrak{p}^n\mathfrak{o}_{\mathfrak{p}}$, and we have only to show that $\mathfrak{p}^{*n}\mathfrak{o}^*_{\mathfrak{p}^*}$ does not contain f. Thus we may assume that $\mathfrak{o}$ is complete.

i) The proof by the theory of multiplicity (This can be applied only for the case where $\mathfrak{o}$ contains a field, because, for the proof of the result in [18] which we want to use, we used the present assertion for the case when $\mathfrak{o}$ does not contain any field): Since $f \notin \mathfrak{m}^n$, the multiplicity of the ring $\mathfrak{o}/f\mathfrak{o}$ is less than n. Since $\mathfrak{o}/f\mathfrak{o}$ is complete, it follows that the multiplicity of the ring $\mathfrak{o}_{\mathfrak{p}}/f\mathfrak{o}_{\mathfrak{p}}$ is less than n (see [18]), which proves that $f \notin \mathfrak{p}^n\mathfrak{o}_{\mathfrak{p}}$.

ii) The proof by quadratic transformation: By Lemma 4.1.2, we may assume that the residue class field of $\mathfrak{o}$ is algebraically closed. On the other hand, making use of an induction argument on the rank of $\mathfrak{o}$, we may asume that co-rank $\mathfrak{p} = 1$. Let $\mathfrak{v}$ be a valuation ring which dominates $\mathfrak{o}$ and which has a prime ideal $\mathfrak{n}$ such that $\mathfrak{v}/\mathfrak{n}$ is algebraic over $\mathfrak{o}/\mathfrak{p}$ and, furthermore, the residue class field of $\mathfrak{v}$ coincides with that of $\mathfrak{o}$ (existence follows from Proposition 2 in Appendix 1 of the present paper). Let v be a valuation whose valuation ring is $\mathfrak{v}$. Then we can select a regular system of parameters $x_1, \cdots, x_r$ of $\mathfrak{o}$ so that $v(x_1) < v(x_j)$ for every $j > 1$. Let $\mathfrak{o}'$ be the quadratic transform of $\mathfrak{o}$ with respect to $\mathfrak{v}$ and set $f' = f/x_1^m$ with m such that $f \in \mathfrak{m}^m$, $f \notin \mathfrak{m}^{m+1}$; we have only to prove that $f' \notin \mathfrak{p}^n\mathfrak{o}_{\mathfrak{p}}$. Repeating successively quadratic transformations, we reach a case where $\mathfrak{p}$ is generated by a subset of a regular system of parameters of $\mathfrak{o}$ (see Appendix 1, § 2) and the assertion is proved.

---

[7] The writer owes the present proof to Prof. Serre.

5. Unique factorization theorem in local rings.

LEMMA 1. *A Noetherian integral domain* $\mathfrak{o}$ *is a unique factorization ring if and only if every prime ideal of rank* 1 *in* $\mathfrak{o}$ *is principal. In this case, an ideal* ($\neq 0, \mathfrak{o}$) *is principal if and only if it is purely of rank* 1 (*that is, each of its prime divisors is of rank* 1).

Proof. 1) Assume that $\mathfrak{o}$ is a unique factorization ring and let $\mathfrak{p}$ be a prime ideal of rank 1. Let a be an irreducible element in $\mathfrak{p}$ (such exists because $\mathfrak{o}$ is Noetherian). If $bc \in \mathfrak{p}$, then by the uniqueness of factorization, one of b and c is divisible by a, which shows that $a\mathfrak{o}$ is prime and $\mathfrak{p} = a\mathfrak{o}$.

2) Assume that every prime ideal of rank 1 is principal. Then every irreducible element generates a prime ideal (of rank 1), from which we see the uniqueness of factorization by induction on the number of irreducible factors.

3) Let $\mathfrak{q}$ be a primary ideal of rank 1 and let $\mathfrak{p}$ be its prime divisor. Then $\mathfrak{p} = a\mathfrak{o}$ ($a \in \mathfrak{o}$). Let n be such that $\mathfrak{q} \subseteq a^n\mathfrak{o}$, $\mathfrak{q} \not\subseteq a^{n+1}\mathfrak{o}$ and set $\mathfrak{q}' = \mathfrak{q} : a^n\mathfrak{o}$. Since $\mathfrak{q} \subseteq a^n\mathfrak{o}$, $\mathfrak{q} = a^n\mathfrak{q}'$. Since $\mathfrak{q} \not\subseteq a^{n+1}\mathfrak{o}$, $\mathfrak{q}' \not\subseteq \mathfrak{p}$. Since by its definition $\mathfrak{q}'$ is of rank 1 unless $\mathfrak{q}' = \mathfrak{o}$, and we have $\mathfrak{q}' = \mathfrak{o}$ and $\mathfrak{q} = a^n\mathfrak{o}$. Now we consider an ideal $\mathfrak{a}$ which is purely of rank 1. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_h$ be the primary components of $\mathfrak{q}$. Then each $\mathfrak{q}_i$ is generated by one element a_i and

$$\mathfrak{a} = a_1(\mathfrak{a} : a_1\mathfrak{o}) = \cdots = a_1 \cdots a_h(\mathfrak{a} : a_1 \cdots a_h\mathfrak{o}) = a_1 \cdots a_h\mathfrak{o}.$$

4) Assume that an ideal $\mathfrak{a}$ is generated by an element a and let $\mathfrak{q}_1, \cdots, \mathfrak{q}_h$ be the primary components of $\mathfrak{a}$ belonging to prime divisors of rank 1. By 3) $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$ is principal: Let b be a generator. Then $\mathfrak{a} = a\mathfrak{o} \subseteq b\mathfrak{o}$ and there exists an element $c \in \mathfrak{o}$ such that $a = bc$. If c is not a unit in $\mathfrak{o}$, then there exists a prime ideal $\mathfrak{p}$ of rank 1 which contains c and we have a contradiction from $b\mathfrak{o}_{\mathfrak{p}} = a\mathfrak{o}_{\mathfrak{p}} \subseteq b\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ (see [16]). Thus $a\mathfrak{o} = b\mathfrak{o}$ and the proof is completed.

Remark 1. By the proofs 3) and 4) above, we see that when $\mathfrak{a}$ is an ideal of a Noetherian integral domain $\mathfrak{o}$ and every minimal prime divisor of $\mathfrak{a}$ is principal, then $\mathfrak{a}$ is principal if and only if $\mathfrak{a}$ is purely of rank 1.

Remark 2. A unique factorization ring $\mathfrak{o}$ is a normal ring. (Gauss' Lemma)

Proof. Every principal ideal of $\mathfrak{o}$ has no imbedded prime divisor. Therefore $\mathfrak{o} = \cap\, \mathfrak{o}_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over all prime ideals of rank 1 in $\mathfrak{o}$ (see [17]). Further, if $\mathfrak{p}$ is a prime ideal of rank 1, then $\mathfrak{p}$ is principal and $\mathfrak{o}_{\mathfrak{p}}$ is a discrete valuation ring. It follows that $\mathfrak{o}$ is normal.

Remark 3. If an integral domain $\mathfrak{o}$ is a unique factorization ring, then every ring of quotients of $\mathfrak{o}$ is also a unique factorization ring.

The proof is easy.

PROPOSITION 8. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be local rings such that* 1) *$\mathfrak{o}$ is a subring of $\mathfrak{o}'$ and* 2) *$a\mathfrak{o}' \cap \mathfrak{o} = a\mathfrak{o}$ for every element $a \in \mathfrak{o}$. Then an ideal $\mathfrak{a}$ of $\mathfrak{o}$ is principal if* (*and only if*) *$\mathfrak{a}\mathfrak{o}'$ is principal.*

Proof. Let b' be an element of $\mathfrak{o}'$ such that $\mathfrak{a}\mathfrak{o}' = b'\mathfrak{o}'$. If there is no element a of $\mathfrak{a}$ such that $a\mathfrak{o}' = b'\mathfrak{o}'$, then $\mathfrak{a}\mathfrak{o}' \subseteq b'\mathfrak{m}'\mathfrak{o}'$, where $\mathfrak{m}'$ is the maximal ideal of $\mathfrak{o}'$. It follows that $b'\mathfrak{o}' = b'\mathfrak{m}'\mathfrak{o}'$, which is impossible unless $b' = 0$ (see [16]). Therefore, there exists an element a of $\mathfrak{a}$ such that $a\mathfrak{o}' = \mathfrak{a}\mathfrak{o}'$, hence $a\mathfrak{o} \subseteq \mathfrak{a} \subseteq a\mathfrak{o}' \cap \mathfrak{o} = a\mathfrak{o}$ and $\mathfrak{a} = a\mathfrak{o}$.

COROLLARY 1. *Let $\mathfrak{o}^*$ be the completion of a local ring $\mathfrak{o}$. Then an ideal $\mathfrak{a}$ of $\mathfrak{o}$ is principal if and only if $\mathfrak{a}\mathfrak{o}^*$ is principal.*

COROLLARY 2. *Assume that a local ring $\mathfrak{o}'$ dominates a local integral domain $\mathfrak{o}$, that no element of $\mathfrak{o}$ is a zero-divisor in $\mathfrak{o}'$ and that $K \cap \mathfrak{o}' = \mathfrak{o}$ with K the field of quotients of $\mathfrak{o}$. Then an ideal $\mathfrak{a}$ of $\mathfrak{o}$ is principal if and only if $\mathfrak{a}\mathfrak{o}'$ is principal.*

THEOREM 3. *Let $\mathfrak{o}^*$ be the completion of a local integral domain $\mathfrak{o}$. If $\mathfrak{o}^*$ is a unique factorization ring, then $\mathfrak{o}$ is also a unique factorization ring.*[8]

Proof. By Lemma 1, we have only to show that every prime ideal $\mathfrak{p}$ of rank 1 in $\mathfrak{o}$ is principal. Let S be the complement of $\mathfrak{p}$ in $\mathfrak{o}$. Since $\mathfrak{o}^*/\mathfrak{p}\mathfrak{o}^*$ is the completion of $\mathfrak{o}/\mathfrak{p}$ (Lemma 0.3), no element of S is a zero-divisor modulo $\mathfrak{p}\mathfrak{o}^*$ (Corollary to Lemma 0.4). If we knew that $\mathfrak{o}$ is a normal ring, then the proof proceeds as follows: $\mathfrak{o}_{\mathfrak{p}}$ is a valuation ring and $\mathfrak{p}\mathfrak{o}^*_S$ is a principal ideal, which shows that every prime divisor of $\mathfrak{p}\mathfrak{o}^*_S$ is of rank 1 (because $\mathfrak{o}^*_S$ is normal or because $\mathfrak{o}^*_S$ is a unique factorization ring). Since no element of S is a zero-divisor modulo $\mathfrak{p}\mathfrak{o}^*$, every prime divisor of $\mathfrak{p}\mathfrak{o}^*$ is of rank 1. Hence $\mathfrak{p}\mathfrak{o}^*$ is principal by Lemma 1 and $\mathfrak{p}$ is principal by Corollary 1 to Proposition 8. Now the proof is completed by the following

---

[8] These results were announced by Mr. Y. Mori at the spring meeting of the Mathematical Society of Japan in 1949. The present proofs were found by the writer independently in March of 1950, which were sketched in [15]. Recently the writer saw that the same results were proved by Krull [9].

LEMMA 2. *Let $\mathfrak{o}^*$ be the completion of a local integral domain $\mathfrak{o}$. If $\mathfrak{o}^*$ is a normal ring, then $\mathfrak{o}$ is also a normal ring.*

But this follows immediately from the following

LEMMA 3. *Let $\mathfrak{o}^*$ be the completion of a semi-local integral domain $\mathfrak{o}$. If K is the field of quotients of $\mathfrak{o}$, then $\mathfrak{o} = K \cap \mathfrak{o}^*$.* (See Nagata [14] or [15].)

Proof. It is obvious that $\mathfrak{o} \subseteq K \cap \mathfrak{o}^*$. We shall prove the converse inclusion. Let a/b $(a, b \in \mathfrak{o})$ be an element of $K \cap \mathfrak{o}^*$. Then $a/b \in \mathfrak{o}^*$ shows that $a \in b\mathfrak{o}^* \cap \mathfrak{o} = b\mathfrak{o}$ (Lemma 0.3) and $a/b \in \mathfrak{o}$.

PROPOSITION 9. *Let $\mathfrak{a}$ be an ideal of a local ring $\mathfrak{o}$. If there exist an ideal $\mathfrak{b}$ of $\mathfrak{o}$ contained in $\mathfrak{a}$ and a non-unit x of $\mathfrak{o}$ such that 1) $\mathfrak{a} : x\mathfrak{o} = \mathfrak{a}$ and 2) $\mathfrak{a} \subseteq \mathfrak{b} + x\mathfrak{o}$, then we have $\mathfrak{a} = \mathfrak{b}$.*[9]

Proof. *Since* $\mathfrak{a} \subseteq \mathfrak{b} + x\mathfrak{o}$, every element a of $\mathfrak{a}$ is expressed in the form $a = b + xz$ with $b \in \mathfrak{b}$, $z \in \mathfrak{o}$. Then $xz \in \mathfrak{a}$ and $z \in \mathfrak{a}$ because $\mathfrak{a} : x\mathfrak{o} = \mathfrak{a}$. Thus $\mathfrak{a} = \mathfrak{b} + x\mathfrak{a}$, which shows that $\mathfrak{a} = \mathfrak{b}$ because x is in the maximal ideal of $\mathfrak{o}$ ([16]).

COROLLARY 1. *Let $\mathfrak{a}$ be an ideal of a local ring $\mathfrak{o}$. If there exists a non-unit x of $\mathfrak{o}$ such that 1) $\mathfrak{a} : x\mathfrak{o} = \mathfrak{a}$ and 2) $\mathfrak{a} \subseteq x\mathfrak{o}$, then $\mathfrak{a} = 0$.*

COROLLARY 2. *Let $\mathfrak{a}$ be an ideal of a local ring $\mathfrak{o}$. If there exists a non-unit x of $\mathfrak{o}$ such that 1) $\mathfrak{a} : x\mathfrak{o} = \mathfrak{a}$ and 2) $\mathfrak{a}$ is principal modulo $x\mathfrak{o}$, then $\mathfrak{a}$ is also principal.*

THEOREM 4. *Let $\mathfrak{o}$ be a regular local ring of rank r. If either $\mathfrak{o}$ is unramified, or r is not greater than 2, then $\mathfrak{o}$ is a unique factorization ring.*[8]

Proof. When $r = 1$, $\mathfrak{o}$ is a discrete valuation ring and our assertion is obvious. Assume next that $r = 2$. Let x be an element of the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$ which is not in $\mathfrak{m}^2$. Let $\mathfrak{p}$ be a prime ideal of rank 1 in $\mathfrak{o}$.

---

[9] If we want to generalize this assertion to general Noetherian rings, then a similar proof shows the following:

Let $\mathfrak{a}$ be an ideal of a Noetherian ring $\mathfrak{o}$ and let $\mathfrak{b}$ be an ideal contained in $\mathfrak{a}$. If there exists an element x of $\mathfrak{o}$ such that 1) $\mathfrak{a} : x\mathfrak{o} = \mathfrak{a}$, 2) $\mathfrak{q} + x\mathfrak{o} \neq \mathfrak{o}$ for every prime divisor $\mathfrak{q}$ of $\mathfrak{b}$ and 3) $\mathfrak{a}$ is contained in $\mathfrak{b} + x\mathfrak{o}$, then we have $\mathfrak{a} = \mathfrak{b}$.

If $x \in \mathfrak{p}$, then $\mathfrak{p} = x\mathfrak{o}$. If $x \notin \mathfrak{p}$, then $\mathfrak{p}$ is principal modulo $x\mathfrak{o}$ because $\mathfrak{o}/x\mathfrak{o}$ is a valuation ring, which shows that $\mathfrak{p}$ is principal by Corollary 2 to Proposition 9 and the assertion is proved in this case. On the other hand, if $\mathfrak{o}$ is unramified, then the completion $\mathfrak{o}^*$ of $\mathfrak{o}$ is a unique factorization ring (Lemma 0.9) and $\mathfrak{o}$ is also a unique factorization ring by Theorem 3.

PROPOSITION 10. *If a regular local ring* $\mathfrak{o}$ *is tamely unramified with respect to a semi-ground ring, then* $\mathfrak{o}$ *is a unique factorization ring.*

Proof. By Theorem 3, we may assume that $\mathfrak{o}$ is complete. Then $\mathfrak{o}$ is isomorphic to a formal power series ring over a ring I, whcih is a field or a discrete valuation ring. Then the proposition is well known in this case (see for example Cohen [6]) and can be proved by induction on the rank of $\mathfrak{o}$ just as in the case of polynomial rings. Therefore, we shall omit the proof. (Cohen's proof can be simplified a little.)

Though it seems to the writer very likely that every regular local ring is a unique factorization ring, the writer cannot prove it yet. But we can prove the following

PROPOSITION 11. *If every regular local ring of rank* 3 *is a unique factorization ring, then so is every regular local ring.*[10]

In order to prove this proposition, we shall prove the following two lemmas:

LEMMA 4. *Assume that* $0 \to A \to B \to C \to 0$ *is an exact sequence of modules* A, B, C *(over a ring* $\mathfrak{o}$*). Then* 1) *if* $\mathrm{dh}\,A > \mathrm{dh}\,B$, *then* $\mathrm{dh}\,A = \mathrm{dh}\,C - 1$; 2) *if* $\mathrm{dh}\,A < \mathrm{dh}\,C - 1$, *or if* $\mathrm{dh}\,A < \mathrm{dh}\,B - 1$, *or if* $\mathrm{dh}\,A < \mathrm{dh}\,B$ *and* $\mathrm{dh}\,A < \mathrm{dh}\,C$, *then* $\mathrm{dh}\,B = \mathrm{dh}\,C$.

Proof. From the exactness of the sequence $0 \to A \to B \to C \to 0$, we have the exactness of the sequence

$$\cdots \to \mathrm{Ext}^{n-1}(A,X) \to \mathrm{Ext}^{n}(C,X) \to \mathrm{Ext}^{n}(B,X) \to \mathrm{Ext}^{n}(A,X)$$
$$\to \mathrm{Ext}^{n+1}(C,X) \to \mathrm{Ext}^{n+1}(B,X) \to \mathrm{Ext}^{n+1}(A,X) \to \cdots$$

with an arbitrary module X, from which the assertion follows immediately.

COROLLARY. *Let* a *and* b *be elements of an integral domain* $\mathfrak{o}$. *If* $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) \neq 0$, *then* $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) = \mathrm{dh}_{\mathfrak{o}}(b\mathfrak{o} + a\mathfrak{o}) - 1$.

---

[10] This result was proved independently by Zariski.

Proof. Since $0 \to b\mathfrak{o} \to a\mathfrak{o} + b\mathfrak{o} \to \mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o}) \to 0$ is exact and since $\mathrm{dh}_{\mathfrak{o}}\, b\mathfrak{o} = 0$, $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) = \mathrm{dh}_{\mathfrak{o}}\, \mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o})$. Since

$$0 \to (a\mathfrak{o} : b\mathfrak{o}) \to \mathfrak{o} \to \mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o}) \to 0$$

is exact, $\mathrm{dh}_{\mathfrak{o}}\, \mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o}) = \mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) + 1$. Thus the assertion is proved.

LEMMA 5. *Let $\mathfrak{o}$ be a regular local ring of rank $r \geqq 3$. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$. Assume that every regular local ring of rank less than r is a unique factorization ring. If a and b are elements of $\mathfrak{m}$ such that $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) \leqq r - 2$, then the ideal $a\mathfrak{o} : b\mathfrak{o}$ is principal.*

Proof. From $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) \leqq r - 2$, *it* follows that either $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) = 0$ or $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) \leqq r - 3$. If $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) = 0$, $a\mathfrak{o} + b\mathfrak{o}$ is principal (because $\mathfrak{o}$ is a local ring), hence either $a\mathfrak{o} \subseteq b\mathfrak{o}$ or $b\mathfrak{o} \subseteq a\mathfrak{o}$ (again by the fact that $\mathfrak{o}$ is a local ring). Therefore, the assertion is easy in this case. In the other case, since $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) \leqq r - 3$, it follows that $\mathrm{dh}_{\mathfrak{o}}\, \mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o}) \leqq r - 2$. This shows that there exists an $\mathfrak{o}/(a\mathfrak{o} : b\mathfrak{o})$-series of length 2, that is, there exists an element $x \in \mathfrak{m}$ which is not a zero-divisor modulo $a\mathfrak{o} : b\mathfrak{o}$ such that $((a\mathfrak{o} : b\mathfrak{o}) + x\mathfrak{o}) : \mathfrak{m} = (a\mathfrak{o} : b\mathfrak{o}) + x\mathfrak{o}$, by Proposition 5. We can select such an x so that $x \notin \mathfrak{m}^2$ (see [19]; cf. [16]). Let $\mathfrak{q}$ be an arbitrary prime divisor of $(a\mathfrak{o} : b\mathfrak{o}) + x\mathfrak{o}$. Since $\mathfrak{o}_{\mathfrak{q}}$ is a regular local ring of rank less than r, $a\mathfrak{o}_{\mathfrak{q}} : b\mathfrak{o}_{\mathfrak{q}}$ is principal and $((a\mathfrak{o} : b\mathfrak{o}) + x\mathfrak{o})\mathfrak{o}_{\mathfrak{q}}$ is generated by two elements. It follows that $\mathfrak{q}$ is of rank 2 by the unmixedness theorem (see Cohen [6] or Nagata [18]), which shows that $((a\mathfrak{o} : b\mathfrak{o}) + x\mathfrak{o})/x\mathfrak{o}$ is purely of rank 1, hence it is principal by Lemma 1. Since x is not a zero-divisor modulo $a\mathfrak{o} : b\mathfrak{o}$, it follows that $a\mathfrak{o} : b\mathfrak{o}$ is principal by Corollary 2 to Proposition 9.

Remark. If $\mathfrak{o}$ is a unique factorization ring, then $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o})$ is not greater than 1 for arbitrary elements a and b of $\mathfrak{o}$.

Proof. If $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) \neq 0$, then $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) = \mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) - 1$. But $a\mathfrak{o} : b\mathfrak{o}$ is purely of rank 1 or is $\mathfrak{o}$ itself, hence it is free and $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} : b\mathfrak{o}) = 0$. It follows that $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o} + b\mathfrak{o}) = 1$ or 0.

Now we shall prove Proposition 11. Let $\mathfrak{o}$ be a regular local ring of rank r; we prove the assertion by induction on r. By our assumption, we may assume that $r \geqq 4$. Let $\mathfrak{p}$ be a prime ideal of rank 1 in $\mathfrak{o}$, and let a and b be elements of $\mathfrak{o}$ such that 1) $a\mathfrak{o}_{\mathfrak{p}} = \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$, 2) $b \notin \mathfrak{p}$, but b is in every primary component of $a\mathfrak{o}$ belonging to a prime divisor other than $\mathfrak{p}$. Then $a\mathfrak{o} : b\mathfrak{o} = \mathfrak{p}$. Let $\mathfrak{a}$ be the ideal such that $\mathfrak{a} = (a\mathfrak{o} : b\mathfrak{o}) : \mathfrak{m}^t$, with t an integer, and $\mathfrak{a} : \mathfrak{m} = \mathfrak{a}$, where $\mathfrak{m}$ is the maximal ideal of $\mathfrak{o}$. Let x be an element of $\mathfrak{m}$

which is not in $\mathfrak{m}^2$ such that $\mathfrak{a}:x\mathfrak{o}=\mathfrak{a}$. By our assumption, $\mathfrak{o}/x\mathfrak{o}$ is a unique factorization ring, and therefore $\mathrm{dh}_{\mathfrak{o}/x\mathfrak{o}}(a\mathfrak{o}+b\mathfrak{o}+x\mathfrak{o})/x\mathfrak{o}$ is not greater than 1. Since r is not less than 4, it follows that $(a\mathfrak{o}+b\mathfrak{o}+x\mathfrak{o}):\mathfrak{m}=a\mathfrak{o}+b\mathfrak{o}+x\mathfrak{o}$ by Proposition 5, which shows that $a\mathfrak{o}+b\mathfrak{o}+x\mathfrak{o}$ contains $\mathfrak{a}$. Since $\mathfrak{a}:x\mathfrak{o}=\mathfrak{a}$, we have $a\mathfrak{o}+b\mathfrak{o}=\mathfrak{a}$ by Proposition 9, which shows that $(a\mathfrak{o}+b\mathfrak{o}):\mathfrak{m}=(a\mathfrak{o}+b\mathfrak{o})$ and $\mathrm{dh}_{\mathfrak{o}}\,\mathfrak{o}/(a\mathfrak{o}+b\mathfrak{o})\leqq r-1$ by Proposition 5, that is, $\mathrm{dh}_{\mathfrak{o}}(a\mathfrak{o}+b\mathfrak{o})\leqq r-2$. Therefore $\mathfrak{p}=a\mathfrak{o}:b\mathfrak{o}$ is principal by Lemma 5, which proves our assertion.

Appendix 1. Rings of Quotients of Regular Local Rings.

1. Some preliminary results.

LEMMA 1. *If $\mathfrak{o}$ is a complete local integral domain, then the derived normal ring $\mathfrak{o}'$ of $\mathfrak{o}$ is a finite $\mathfrak{o}$-module.* (Nagata [14]).

Proof. Since $\mathfrak{o}$ is complete, there exists a complete regular local ring $\mathfrak{r}$ such that $\mathfrak{o}$ is a finite $\mathfrak{r}$-module (Lemma 0.8). Therefore, we have only to prove the following

LEMMA 2. *Let $\mathfrak{r}$ be a complete regular local ring, and let L be a finite algebraic extension of the field of quotients K of $\mathfrak{r}$. Then the integral closure $\mathfrak{o}$ of $\mathfrak{r}$ in L is a finite $\mathfrak{r}$-module.*

Proof. If $\mathfrak{r}$ is of characteristic zero, then L is separable over K and our assertion is obvious ([16, § 5]). Therefore, we assume that L is of characteristic $p\neq 0$. Then we may assume that $\mathfrak{r}$ is the ring of formal power series in indeterminates $x_1,\cdots,x_n$ over a field $\boldsymbol{k}$ (Lemma 0.10). Let L' be a purely inseparable finite algebraic extension of K such that $L(L')$ is separable over L'. If we know that the integral closure $\mathfrak{o}'$ of $\mathfrak{r}$ in L' is a finite $\mathfrak{r}$-module, then the integral closure $\mathfrak{o}''$ of $\mathfrak{r}$ in $L(L')$ is a finite $\mathfrak{r}$-module because $L(L')$ is separable over L', and $\mathfrak{o}$ is also finite $\mathfrak{r}$-module. Thus, we may assume that L is purely inseparable over K. Set $e=[L:K]$, $\mathfrak{k}=\boldsymbol{k}^{1/e}$, $y_i=x_i^{1/e}$ $(i=1,\cdots,n)$ and $\mathfrak{r}^*=\mathfrak{k}\{y_1,\cdots,y_n\}$. Then $\mathfrak{o}$ is a subring of $\mathfrak{r}^*$ because $\mathfrak{r}^*$ is regular and hence normal, so that an element a of $\mathfrak{o}$ can be expressed as a power series in $y_1,\cdots,y_n$ with coefficients in $\mathfrak{k}$. The leading form of the expression will be called the leading form of a in the present proof.

LEMMA 3. *If $f_1,\cdots,f_m$ are leading forms of elements $a_1,\cdots,a_m$ of $\mathfrak{o}$ respectively, and if $1,f_1,\cdots,f_m$ are linearly independent over $\mathfrak{r}$, then $1,a_1,\cdots,a_m$ are linearly independent over $\mathfrak{r}$.*

Proof. We consider a linear combination $\sum a_ib_i$ ($b_i \in \mathfrak{r}$). Let g_i be the leading form of b_i. Then f_ig_i is the leading form of a_ib_i. We may assume that $\deg(f_1g_1) = \cdots = \deg(f_rg_r) = d$ and that $\deg(f_ig_i) > d$ for $i > r$. Then the leading form of $\sum a_ib_i$ is $\sum_1^r f_ig_i$, which is not in $\mathfrak{r}$ because $1, f_1, \cdots, f_r$ are linearly independent over $\mathfrak{r}$. Therefore $\sum a_ib_i \notin \mathfrak{r}$ unless all the b_i's are zero, which proves Lemma 4.

Now we proceed with the proof of Lemma 2. Since L is finite over K, there are leading forms $f_1, \cdots, f_s$ of elements of $\mathfrak{o}$ such that $1, f_1, \cdots, f_s$ is a maximal linearly independent set of leading forms of elements of $\mathfrak{o}$ by Lemma 3. Let $c_1, \cdots, c_t$ be the coefficients of $f_1, \cdots, f_s$ and let f be the leading form of an element of $\mathfrak{o}$. Since f is linearly dependent on $1, f_1, \cdots, f_s$ over $\mathfrak{r}$, it follows that the coefficients of f are in $\boldsymbol{k}(c_1, \cdots, c_t)$. Now let $d_0 = 1, d_1, \cdots, d_u$ be a linear base of $\boldsymbol{k}(c_1, \cdots, c_t)$ over $\boldsymbol{k}$ and let $m_0 = 1, m_1, \cdots, m_v$ be the set of monomials in $y_1, \cdots, y_n$ of degree less than *one*. Then f is contained in the module generated by all the d_im_j over $\mathfrak{r}$. Therefore, there exist elements $a_1, \cdots, a_w$ of $\mathfrak{o}$ such that the leading form of every element of $\mathfrak{o}$ is contained in the $\mathfrak{r}$-module generated by the leading forms of $a_1, \cdots, a_w$. Since $\mathfrak{r}[a_1, \cdots, a_w]$ is a finite $\mathfrak{r}$-module, it is a complete local integral domain (Lemma 0. 5). Since $\mathfrak{r}^*$ dominates $\mathfrak{r}[a_1, \cdots, a_w]$, $\mathfrak{r}[a_1, \cdots, a_w]$ is a subspace of $\mathfrak{r}^*$ (Lemma 0. 11). On the other hand, by our choice of $a_1, \cdots, a_w$, we see that $\mathfrak{o}$ is contained in $\mathfrak{r}[a_1, \cdots, a_w] + \mathfrak{m}^{*i}$ for every natural number i, where $\mathfrak{m}^*$ denotes the maximal ideal of $\mathfrak{r}^*$. Since $\mathfrak{r}[a_1, \cdots, a_w]$ is complete and is a subspace of $\mathfrak{r}^*$, it must be a closed set of $\mathfrak{r}^*$. Therefore, we have $\mathfrak{o} \subseteq \mathfrak{r}[a_1, \cdots, a_w]$ and $\mathfrak{r}[a_1, \cdots, a_w] = \mathfrak{o}$. Thus the proof is completed.

COROLLARY 1. *Every complete local integral domain satisfies the finiteness conditions for integral extensions.*

COROLLARY 2. *If a complete semi-local ring $\mathfrak{o}$ has no nilpotent elements, then the integraly closure of $\mathfrak{o}$ in its total quotient ring is a finite $\mathfrak{o}$-module.*

PROPOSITION 1. *If a semi-local integral domain $\mathfrak{o}$ is analytically unramified, then the derived normal ring $\mathfrak{o}'$ of $\mathfrak{o}$ is a finite $\mathfrak{o}$-module.* (Nagata [11])

Proof. Let $\mathfrak{o} = \mathfrak{o}_0 \subseteq \mathfrak{o}_1 \subseteq \cdots \subseteq \mathfrak{o}_n \subseteq \cdots$ be a chain of subrings of $\mathfrak{o}'$ such that each $\mathfrak{o}_i$ is a finite $\mathfrak{o}$-module. Then the completions $\mathfrak{o}^*_i$ of the rings $\mathfrak{o}_i$ can be imbedded in the integral closure $\mathfrak{o}^{*\prime}$ of the completion $\mathfrak{o}^*$ of $\mathfrak{o}$ (Lemma 0. 6). Since $\mathfrak{o}^*$ has no nilpotent elements, $\mathfrak{o}^{*\prime}$ is a finite $\mathfrak{o}^*$-module and there exists an i such that $\mathfrak{o}^*_i = \mathfrak{o}^*_j$ for every $j > i$. Then we have $\mathfrak{o}_i = \mathfrak{o}_j$ ($j > i$) by Lemma 4. 5. 3. Thus $\mathfrak{o}'$ is a finite $\mathfrak{o}$-module.

Proposition 2. *Let* $\mathfrak{o}$ *be a Noetherian integral domain and let* L *be a finite algebraic extension of the field of quotients of* $\mathfrak{o}$. *If* $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ *are prime ideals of* $\mathfrak{o}$ *such that* $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$, *then there exists a valuation ring* $\mathfrak{v}$ *of* L *which has prime ideals* $\mathfrak{n}_1, \cdots, \mathfrak{n}_n$ *such that* 1) $\mathfrak{v}_{\mathfrak{n}_i}$ *dominates* $\mathfrak{o}_{\mathfrak{p}_i}$ *and* 2) $\mathfrak{v}_{\mathfrak{n}_i}/\mathfrak{n}_i$ *is a finite algebraic extension of* $\mathfrak{o}_{\mathfrak{p}_i}/\mathfrak{p}_i\mathfrak{o}_{\mathfrak{p}_i}$ *(for each* i*).*

Proof. We may assume that $\mathfrak{p}_n$ is of rank 1. Let $\mathfrak{o}'$ be the integral closure of $\mathfrak{o}_{\mathfrak{p}_n}$ in L. Then $\mathfrak{o}'$ is a Dedekind domain by Lemma 0.15. Let $\mathfrak{p}'$ be a maximal ideal of $\mathfrak{o}'$. Then $\mathfrak{o}'_{\mathfrak{p}'}$ is a valuation ring and $\mathfrak{o}'_{\mathfrak{p}'}/\mathfrak{p}'\mathfrak{o}'_{\mathfrak{p}'}$ is a finite algebraic extension of $\mathfrak{o}_{\mathfrak{p}_n}/\mathfrak{p}_n\mathfrak{o}_{\mathfrak{p}_n}$ by Lemma 0.15. The rest of the proof is like the proof of Proposition 1.5.

Remark. If $\mathfrak{o}$ is a regular local ring, then there exists a valuation ring of the field of quotients of $\mathfrak{o}$ which dominates $\mathfrak{o}$ and whose residue class field coincides with that of $\mathfrak{o}$.

Proof. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$ and let f be an element of $\mathfrak{m}$ which is not in $\mathfrak{m}^2$. Then $\mathfrak{o}/f\mathfrak{o}$ is a regular local ring and $\mathfrak{o}_{f\mathfrak{o}}$ is a valuation ring. Therefore, our assertion is easily proved by induction on the rank of $\mathfrak{o}$.

2. A proof of Theorem 1 in some special cases.

Lemma 1. *Let* $\mathfrak{o}$ *be a regular local ring of rank* r *and let* $\mathfrak{p}$ *be a prime ideal of co-rank* 1 *in* $\mathfrak{o}$. *If the derived normal ring of* $\mathfrak{o}/\mathfrak{p}$ *is a finite* $\mathfrak{o}/\mathfrak{p}$-*module, then* $\mathfrak{o}_{\mathfrak{p}}$ *is a regular local ring of rank* $r-1$. (Zariski [26])

Proof. Let $\mathfrak{v}$ be a valuation ring which dominates $\mathfrak{o}$ and has a prime ideal $\mathfrak{n}$ such that $\mathfrak{n} \cap \mathfrak{o} = \mathfrak{p}$ and $\mathfrak{v}/\mathfrak{n}$ is algebraic over $\mathfrak{o}/\mathfrak{p}$ (existence of $\mathfrak{v}$ follows from Proposition 2). Let $\mathfrak{o}_1, \cdots, \mathfrak{o}_n, \cdots$ be successive quadratic transforms of $\mathfrak{o}$ with respect to $\mathfrak{v}$ (that is, $\mathfrak{o}_1$ is the quadratic transform of $\mathfrak{o}$ with respect to $\mathfrak{v}$, $\mathfrak{o}_2$ is that of $\mathfrak{o}_1$ and so on). Then by Proposition 4.4, each $\mathfrak{o}_i$ is a regular local ring and has a prime ideal $\mathfrak{p}_i$ such that $\mathfrak{o}_{\mathfrak{p}} = (\mathfrak{o}_i)_{\mathfrak{p}_i}$ ($\mathfrak{p}_i = \mathfrak{n} \cap \mathfrak{o}_i$). Let $\mathfrak{o}'$ be the derived normal ring of $\mathfrak{o}/\mathfrak{p}$ and set $\mathfrak{m}' = (\mathfrak{m}/\mathfrak{n}) \cap \mathfrak{o}'$, where $\mathfrak{m}$ is the maximal ideal of $\mathfrak{v}$. Then, as is easily seen, $\mathfrak{o}_i/\mathfrak{p}_i$ is contained in $\mathfrak{o}'_{\mathfrak{m}'}$ for every i. Since $\mathfrak{o}'$ is finite over $\mathfrak{o}/\mathfrak{p}$, there exists an n such that $\mathfrak{o}_n/\mathfrak{p}_n = \mathfrak{o}_{n+1}/\mathfrak{p}_{n+1}$. Since $\mathfrak{o}_{n+1}/\mathfrak{p}_{n+1}$ is the quadratic transform of $\mathfrak{o}_n/\mathfrak{p}_n$ with respect to $\mathfrak{v}/\mathfrak{n}$, it follows that $\mathfrak{o}_n/\mathfrak{p}_n$ is a discrete valuation ring. Hence $\mathfrak{p}_n$ is generated by $r-1$ elements (Lemma 0.12) and $\mathfrak{o}_{\mathfrak{p}} = (\mathfrak{o}_n)_{\mathfrak{p}_n}$ is a regular local ring of rank $r-1$, which proves the assertion.

Making use of an induction argument on the rank of a regular local ring, we easily see the following fact:

Let $\mathfrak{o}$ be a regular local ring and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$. If there exist prime ideals $\mathfrak{p} = \mathfrak{p}_t \subset \mathfrak{p}_{t-1} \subset \cdots \subset \mathfrak{p}_0$ such that each $\mathfrak{p}_i$ is of co-rank i and the derived normal ring of $\mathfrak{o}_{\mathfrak{p}_{i-1}}/\mathfrak{p}_i\mathfrak{o}_{\mathfrak{p}_{i-1}}$ is a finite module over the latter ring for every i, then $\mathfrak{o}_{\mathfrak{p}}$ is a regular local ring.

As consequences of the above result, we have

(1) If $\mathfrak{o}$ is a complete regular local ring, then $\mathfrak{o}_{\mathfrak{p}}$ is a regular local ring for every prime ideal $\mathfrak{p}$ of $\mathfrak{o}$.

(See Lemma 1 in § 1.)

(2) If P is a simple spot in the restricted case, then $P_{\mathfrak{p}}$ is a regular local ring for every prime ideal $\mathfrak{p}$ of P.

Appendix 2. Some Remarks on the Non-restricted Case.

PROPOSITION 1. *Let P be a local ring which dominates a discrete valuation ring $\mathfrak{v}$, and let $\mathfrak{v}^*$ be a valuation ring which contains $\mathfrak{v}$ as a dense subspace. Let $\mathfrak{m}$ be the maximal ideal of P and set $R = \mathfrak{v}^* \otimes_{\mathfrak{v}} P$, $\mathfrak{m}' = \mathfrak{m}R$. Then $\mathfrak{m}'$ is a maximal ideal of R. Set $P' = R'_{\mathfrak{m}'}$. If P' is Noetherian, then P' is a local ring which contains P as a dense subspace.*

Proof. Let $\mathfrak{p}$ be the maximal ideal of $\mathfrak{v}$ and set $\mathfrak{p}^{(i)} = \mathfrak{m}^i \cap \mathfrak{v}$, $\mathfrak{p}^{*(i)} = \mathfrak{p}^{(i)}\mathfrak{v}^*$. Then

$$R/\mathfrak{m}^i R = (\mathfrak{v}^*/\mathfrak{p}^{*(i)}) \otimes_{\mathfrak{v}/\mathfrak{p}^{(i)}} (P/\mathfrak{m}^i) = (\mathfrak{v}/\mathfrak{p}^{(i)}) \otimes (P/\mathfrak{m}^i) = P/\mathfrak{m}^i$$

for every natural number i. Therefore, by the case $i = 1$, we see that $\mathfrak{m}'$ is a maximal ideal of R. If P' is Noetherian, then P' is a local ring. Therefore, $P'/\mathfrak{m}'^i P' = P/\mathfrak{m}^i$ shows that P' contains P as a dense subspace.

COROLLARY. *If P is a spot over a ground ring $\mathfrak{v}$ which is a valuation ring, then P' as defined above is a local ring which contains P as a dense subspace.*

Proof. Let $\mathfrak{o}$ be an affine ring which has a prime ideal $\mathfrak{p}$ such that $P = \mathfrak{o}_{\mathfrak{p}}$. Then R is a ring of quotients of $\mathfrak{v}^* \otimes \mathfrak{o}$, and this last ring is finitely generated over $\mathfrak{v}^*$. It follows that R is Noetherian and P' is also Noetherian.

PROPOSITION 2. *Let P be a spot over a ground ring I. If P is separably generated over I, then P is analytically unramified.*

Proof. Let L be the field of quotients of P and let I' be the integral closure of I in L. Since L is separably generated over I, I' is separable over I and I' is a finite I-module. Set $P' = P[I']$. Then P' is a semi-local integral domain and P is a subspace of P' (Lemma 0.6). Therefore, we have only to show that P' is analytically unramified. Since the completion of P' is the direct sum of completions of local rings (spots) $P'_{\mathfrak{m}'}$, where $\mathfrak{m}'$ runs over all maximal ideals of P' (Lemma 0.2), we have only to show that $P'_{\mathfrak{m}'}$ is analytically unramified. Thus we may assume that P contains I'. Since I' is also a Dedekind domain, we may assume that $I = I'$, and we may assume further that I is the ground place of I dominated by P. If I is a field, then P is a spot in the restricted case, and therefore we assume that I is a discrete valuation ring. Let I^* be the completion of I and set $R = I^* \otimes_I P$, $\mathfrak{n} = \mathfrak{m}R$, $P'' = R_{\mathfrak{n}}$ (see Projosition 1). By the Corollary to Proposition 1, P'' is a local ring which contains P as a dense subspace. Since P is a regular extension of I, R is an integral domain by Theorem 3.3, whence P'' is a spot over I^* (by the proof of the Corollary to Proposition 1). Since I^* is complete, it satisfies the finiteness condition for integral extensions, hence P'' is a spot in the restricted case and P'' is analytically unramified. Since P'' contains P as a dense subspace, we see that P is also analytically unramified.

COROLLARY. *If a spot P is separably generated over a ground ring I, then the derived normal ring of P is a finite P-module.*

This follows from Proposition 1 in Appendix 1 and the above proposition.

PROPOSITION 3. *The completion of a normal spot is an integral domain.*

Proof. (1) We first prove the assertion under the assumption that the spot P is analytically unramified. Let L be the field of quotients of P and let I' be the integral closure of I in L. Since P is normal, I' is contained in P, and therefore we may assume that $I = I'$ (because I' is a Dedekind domain by Lemma 0.15). Thus we assume that the field of quotients K of I is algebraically closed in L. We may also assume that I is a discrete valuation ring dominated by P. Let I^* be the completion of I and K^* be the field of quotients of I^*. Let K' be a maximal separably generated extension of K contained in K^* and set $I' = I^* \cap K'$. Then I' is a valuation ring which contains I as a dense subspace. Set $R = I^* \otimes_I P$, $R' = I' \otimes_I P$, $\mathfrak{n} = \mathfrak{m}R$, $\mathfrak{n}' = \mathfrak{m}R'$, $P'' = R_{\mathfrak{n}}$ and $P' = R'_{\mathfrak{n}'}$, where $\mathfrak{m}$ is the maximal ideal of P (see Proposition 1). Since I' is separably generated over I and since K is algebraically closed in L, R' is an integral domain by Theorem 3.2. Let x be a prime element of I. Then by Lemma 3.6.1, $R'[1/x]$ is a normal ring. $R'/xR' = (I'/xI') \otimes_{I/xI} (P/xP) = P/xP$. Since P is a normal ring, xP has no imbedded prime divisor and xR' has no imbedded prime divisor. Let $\mathfrak{p}'$ be a (minimal) prime divisor of xR' and set $\mathfrak{p} = \mathfrak{p}' \cap P$. Then the fact that $R'/xR' = P/xP$ shows that $\mathfrak{p}$ is a prime divisor of xP. Let S be the complement of $\mathfrak{p}$ in P. Then $R'_S = I' \otimes_I P_S$ and $P_S = P_{\mathfrak{p}}$. Since P is normal, $P_{\mathfrak{p}}$ is a discrete valuation ring. On the other hand, $\mathfrak{p}R'_S$ is a maximal ideal of R'_S and $(R'_S)_{(\mathfrak{p}R'_S)} = R'_{\mathfrak{p}'}$ contains $P_{\mathfrak{p}}$ as a dense subspace by the Corollary to Proposition 1. Therefore $R'_{\mathfrak{p}'}$ is a valuation ring. Therefore, we see that R' is a normal ring ([16]). Now, since I^* is purely inseparable over I', I^* is integral over I' and the zero ideal of R is a primary ideal. Since P'' contains P as a dense subspace and since the completion of P contains no nilpotent elements, we see that P'' is an integral domain and P'' is a spot over I^*. Since I^* is purely inseparable over I' and since P' is a normal ring, the derived normal ring of P'' has only one maximal ideal. Since P'' is a spot in the restricted case, it follows that the completion of P'' is an integral domain. Since P'' contains P as a dense subspace, we see the assertion in this case.

(2) Now we have only to prove that P is analytically unramified. To do this, we shall prove a lemma due to Zariski [27]:

LEMMA 1. *Let $\mathfrak{o}$ be a normal local ring. If there exists a non-unit a of $\mathfrak{o}$ such that every prime divisor of $a\mathfrak{o}$ is analytically unramified, then $\mathfrak{o}$ is analytically unramified.*

Proof. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be the prime divisors of $a\mathfrak{o}$ (they are of rank 1 because $\mathfrak{o}$ is normal), and let $\mathfrak{p}^*_{i1}, \cdots, \mathfrak{p}^*_{i,n(i)}$ be the prime divisors of $\mathfrak{p}_i\mathfrak{o}^*$ for each i; here $\mathfrak{o}^*$ denotes the completion of $\mathfrak{o}$. If S is the intersection of the complements of $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ in $\mathfrak{o}$, then $\mathfrak{o}_S$ is a principal ideal ring ([16]); let x_i be an element of $\mathfrak{o}$ such that $\mathfrak{p}_i\mathfrak{o}_S = x_i\mathfrak{o}_S$ for each i. Then by assumption, $x_i\mathfrak{o}^*_S = \bigcap_j \mathfrak{p}^*_{ij}\mathfrak{o}^*_S$. Since no element of S is a zero-divisor modulo $a\mathfrak{o}^*$, we see that $a\mathfrak{o}^*$ has no prime divisor other than the $\mathfrak{p}^*_{ij}$'s. If $\mathfrak{P}^*_{ij}$ denotes the kernel of the natural homomorphism from $\mathfrak{o}^*$ into $\mathfrak{o}^*_{\mathfrak{p}^*_{ij}}$, the primary component of $a\mathfrak{o}^*$ belonging to $\mathfrak{p}^*_{ij}$ contains $\mathfrak{P}^*_{ij}$ so that $a\mathfrak{o}^*$ contains the intersection $\mathfrak{d}$ of the $\mathfrak{P}^*_{ij}$'s. Since the same holds with a replaced by any power of a, we see that $\mathfrak{d} = 0$. Since $\mathfrak{P}^*_{ij}$ is a prime ideal by Lemma 1.4.1, we see that $\mathfrak{d}$ is a semi-prime ideal and $\mathfrak{o}$ is analytically unramified.

Now we shall return to the proof of Proposition 3. Let x be the same as in part (1) of the proof. Then for every prime divisor $\mathfrak{p}$ of xP, $P/\mathfrak{p}$ is a spot over the field I/xI, is in the restricted case, and is analytically unramified. Therefore, Lemma 1 shows that P is analytically unramified, which completes the proof.

PROPOSITION 4. *If an affine ring* $\mathfrak{o}$ *is separably generated over a ground ring* I, *then the derived normal ring of* $\mathfrak{o}$ *is a finite* $\mathfrak{o}$*-module.*

Proof. Using the Corollary to Proposition 2, we prove the assertion in the same way as in Theorem 1.3.

Once this proposition is proved, we see the existence of the derived normal model of a model in the same way as in Chapter 2 when the function field is separably generated. (For the projective model, observe that the field of quotients of the homogeneous coordinate ring is obtained by adjoining a transcendental element to the function field of the model under the consideration and the separable generation is preserved.)

Now the other assertions in Chapter 2 can be generalized easily for function fields which are separably generated over a ground ring.

Observe here that even when the function field of a model is separably generated over the ground ring, the function field of the induced model of the model defined by a spot may not be separably generated.

MATHEMATICAL INSTITUTE,
KYÔTO UNIVERSITY, JAPAN.

REFERENCES.

[1] N. Bourbaki, *Algèbre*, Chapter III (Algèbre multilinéaire), Paris, Hermann, 1948.

[2] E. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1955.

[3] C. Chevalley, "On the theory of local rings," *Annals of Mathematics*, vol. 44 (1943), pp. 690-708.

[4] ———, "Intersections of algebraic and algebroid varieties," *Transactions of the American Mathematical Society*, vol. 57 (1945), pp. 1-85.

[5] ———, "La notion d'anneau de décomposition," *Nagoya Mathematical Journal*, vol. 7 (1954), pp. 21-33.

[6] I. S. Cohen, "On the structure and ideal theory of compelte local rings," *Transactions of the American Mathematical Society*, vol. 59 (1946), pp. 54-106.

[7] ———, "Commutative rings with restricted minimum condition," *Duke Mathematical Journal*, vol. 17 (1950), pp. 27-42.

[8] W. Krull, "Dimensionstheorie in Stellenringen," *Journal für die Reine und Angewandte Mathematik*, vol. 179 (1938), pp. 208-226.

[9] ———, "Zur Theorie der Kommutativen Integritätsbereiche," *Journal für die Reine und Angewandte Mathematik*, vol. 192 (1953), pp. 230-252.

[10] T. Matsusaka, "The theorem of Bertini on linear systems in modular fields," *Memoirs of the College of Science, University of Kyoto*, ser. A, vol. 26, No. 1 (1950), pp. 51-62.

[11] M .Nagata, "On the structure of complete local rings," *Nagoya Mathematical Journal*, vol. 1 (1950), pp. 63-70; Corrections, vol. 5 (1953), pp. 145-147.

[12] ———, "On the theory of Henselian rings," *ibid.*, vol. 5 (1953), pp. 45-57.

[13] ———, "On the theory of Henselian rings, II," *ibid.*, vol. 7 (1954), pp. 1-19.

[14] ———, "Some remarks on local rings, II," *Memoirs of the College of Science, University of Kyoto*, ser. A, vol. 28, No. 2 (1954), pp. 109-120.

[15] ———, "Local rings, I," *Sûgaku*, vol. 5, No. 2 (1953), pp. 104-114 (in Japanese).

[16] ———, "Basic theorems on general commutative rings," *Memoirs of the College of Science, University of Kyoto*, ser. A, vol. 29, No. 1 (1955), pp. 59-77.

[17] ———, "A general theory of algebraic geometry over Dedekind domains, I," *American Journal of Mathematics*, vol. 78 (1956), pp. 78-116.

[18] ———, "The theory of multiplicity in general local rings," forthcoming.

[19] ———, "On the derived normal rings of Noetherian integral domains," *Memoirs of the College of Science, University of Kyoto*, ser. A, vol. 29, No. 3 (1955), pp. 293-303.

[20] M. Narita, "On the structure of complete local rings," forthcoming.

[21] P. Samuel, "Algèbre local," *Mémorial des Sciences Mathématiques*, No. 123 (1953).

[22] J-P. Serre, "Sur la dimension homologiques des anneaux et des modules noethériens," forthcoming.

[23] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[24] A. Weil, *Foundations of algebraic geometry*, American Mathematical Society Colloquium Publications, 1946.

[25] O. Zariski, "Pencils on an algebraic variety and a new proof of a theorem of Bertini," *Transactions of the American Mathematical Society*, vol. 50 (1941), pp. 48-70.

[26] ———, "The concept of simple points of an abstract algebraic variety," *ibid.*, vol. 62 (1947), pp. 1-52.

[27] ———, "Analytical irreducibility of normal varieties," *Annals of Mathematics*, vol. 49 (1948), pp. 352-361.

Added in Proof. [20] appeared in the *Journal of Mathematical Society of Japan*, vol. 7 (1955) and [18] and [22] appeared in the *Proceedings of International Symposium on Algebraic Number Theory*, Tokyo-Nikko 1955 (1956).

LOCAL UNIQUENESS, EXISTENCE IN THE LARGE, AND THE CONVERGENCE OF SUCCESSIVE APPROXIMATIONS.*

By Fred Brauer and Shlomo Sternberg.

1. It has been remarked by several authors that there is a close analogy between theorems assuring existence in the large of ordinary differential equations on the one hand and local uniqueness theorems on the other, cf. [2], [5], [8], [9]. For example, the majorization principle of Wintner [9] is the counterpart of Kamke's "allgemeine Eindeutigkeitssatz," and Wintner's criterion [8] corresponds to Osgood's uniqueness criterion. Furthermore, these criteria all have analogues which assure the convergence of successive approximations; cf. [7], where the Osgood criterion is shown to suffice, and [3], [1], where the same is shown for the Kamke condition (the additional monotony assumption being superfluous, as will be shown). This second situation is somewhat unsatisfactory, as we know that uniqueness of solutions and the convergence of the successive approximations are logically independent. In fact, Müller, in [6], gives an example of a differential equation which has a unique solution and yet the successive approximations do not converge, and we shall present below an example, due to Dieudonné, of a differential equation such that the successive approximations converge for an arbitrary initial curve and yet the solution is not unique. In the present paper we shall give a uniqueness criterion which includes Kamke's as a special case and is sufficiently general so as not to imply the convergence of successive approximations. We shall also explain the source of the duality between local uniqueness and global existence by showing that global existence can be viewed as a sort of uniqueness theorem at infinity.

2. We first consider the uniqueness of solutions of

$$x'(t) = f(x,t), \qquad x(0) = 0, \tag{1}$$

where x and f are n-dimensional vectors.

Let $V(x,t)$ be a function, defined for vectors x and real t, with non-negative real values, which is continuous in (x,t), has one-sided partial

---

* Received November 22, 1957.

derivatives with respect to t and the components of x, and such that $V(x,t)=0$ implies $x=0$. We will use V_t to denote a partial derivative of V with respect to t, V_x to denote some gradient vector of V, and $\cdot$ to denote the usual scalar product of vectors. Any condition which involves V_x or V_t will be understood to be required for all one-sided derivatives.

THEOREM 1. *Let $\omega(r,t)$ be a continuous non-negative function defined on $r \geqq 0$, $0<t<a$. Suppose the only solution of*

$$r'(t)=\omega(r,t) \tag{2}$$

which satisfies

$$r(0)=r'(0)=0 \tag{3}$$

on $0 \leqq t \leqq \alpha$, for any α in $0<\alpha<a$, is the identically zero solution. Let $f(x,t)$ be continuous on a bounded region $0<t<a$, $V(x,t)<b$ and

$$V_t(x-y,t)+V_x\cdot[f(x,t)-f(y,t)] \leqq \omega[V(x-y,t),t] \tag{4}$$

in this region. Then there is at most one solution of (1) *on $0 \leqq t<a$.*

Proof. Suppose $x_1(t)$ and $x_2(t)$ are two solutions of (1) on $0 \leqq t<a$, and let $y(t)=x_2(t)-x_1(t)$. Then

$$(d/dt)[y^i(t)]=f^i[x_2(t),t]-f^i[x_1(t),t], \tag{5}$$

where the superscript i denotes the i-th component. Let $m(t)=V[y(t),t]$, and $m^*(t)=\limsup_{h\to 0}[m(t)-m(t-h)]/h$. Then

$$\begin{aligned}[m(t)-m(t-h)]/h=\sum_{i=1}^{n}(V[y^1(t),\cdots,y^{i+1}(t-h),\cdots,y^n(t-h),t]\\ -V[y^1(t),\cdots,y^i(t-h),\cdots,y^n(t-h),t])/h\\ +[V(x(t-h),t)-V(x(t-h),t-h)]/h.\end{aligned}$$

Since V has one-sided partial derivatives, this is bounded above by a sum of the form

$$[V_{x^i}(y(t),t)+\epsilon_i][y^i(t)-y^i(t-h)]/h+V_t(y(t),t)+\epsilon_{n+1},$$

where V_{x^i} stands for a suitable one-sided partial derivative of V with respect to x^i, V_t stands for a suitable one-sided partial derivative of V with respect to t, and the ϵ_i tend to zero as $h\to 0$. Letting $h\to 0$, we obtain, using (4), (5), and the continuity of ω,

$$m^*(t) \leqq \omega[m(t),t]. \tag{6}$$

Suppose there exists $\sigma, 0 < \sigma \leqq a$, such that $m(\sigma) > 0$. There is a minimum solution $r(t)$ of (2) through the point $(\sigma, m(\sigma))$, existing on some interval to the left of σ.

As far to the left of σ as $r(t)$ exists, it satisfies

$$0 < r(t) \leqq m(t). \tag{7}$$

To prove this, we first note that $r(t)$ must remain strictly positive, for if $r(t)$ vanishes at a point it can be continued to the interval $0 < t \leqq \sigma$ as a solution of (2), (3), and therefore $r(t)$ must vanish identically by hypothesis. Next, we observe that

$$r'(t) = \omega(r, t) + \epsilon, \qquad r(\sigma) = m(\sigma) \tag{8}$$

has solutions $r(t, \epsilon)$ for all sufficiently small $\epsilon > 0$, existing as far to the left of σ as $r(t)$ exists, and $\lim_{\epsilon \to 0+} r(t, \epsilon) = r(t)$ ([4], p. 83). Thus, it suffices to prove

$$r(t, \epsilon) \leqq m(t) \tag{9}$$

for all $\epsilon > 0$ and all solutions of (8). If this inequality does not hold, there is a least upper bound ζ of numbers $t \leqq \sigma$ for which (9) is false. Since $m(\sigma) = r(\sigma) = r(\sigma, \epsilon)$, and the functions $m(t), r(t, \epsilon)$ are continuous,

$$m(\zeta) = r(\zeta, \epsilon), \qquad m^*(\zeta) \geqq r'(\zeta, \epsilon). \tag{10}$$

Then $\omega(m(\zeta), \zeta) + \epsilon = \omega(r(\zeta, \epsilon), \zeta) + \epsilon = r'(\zeta, \epsilon) \leqq m^*(\zeta) \leqq \omega(m(\zeta), \zeta)$, using (6), (8), (10). This contradiction proves (9), which, as we have remarked, implies (7).

Now $r(t)$ can be continued to the whole interval $0 < t \leqq \sigma$ as a solution of (2) which satisfies (7). Since $\lim_{t \to 0+} m(t) = 0$, $\lim_{t \to 0+} r(t) = 0$, and we may define $r(0) = 0$. If $\| x \|$ denotes the Euclidean norm of a vector x, then by the continuity of f at the origin, there exists $\delta > 0$ such that

$$\| x_2(t) - x_1(t) \| = \| \int_0^t [f(x_2(s), s) - f(x_1(s), s)] ds \| < \eta t,$$

when $0 \leqq t < \delta$, for any $\eta > 0$. By the continuity of V, this implies that given any $\epsilon > 0$, there exists $\delta > 0$ such that $V[x_2(t) - x_1(t), t] < \epsilon t$ for $0 \leqq t < \delta$. This implies $0 < m(t)/t < \epsilon$ for $0 < t < \delta$, and $\lim_{t \to 0+} m(t)/t = 0$, which proves $r'(0) = 0$. Thus $r(t)$ is a solution of (2) which satisfies (3), and by hypothesis, $r(t)$ must vanish identically on $0 \leqq t \leqq \sigma$, contradicting the choice of $r(\sigma)$. Hence $x_1(t) = x_2(t)$ on $0 \leqq t < a$, which is the desired uniqueness result.

Instead of a single function $V(x,t)$, we may use a vector-valued function $\nu(x,t)$, and require that (4) be satisfied for each component of $\nu(x,t)$. Instead of requiring $x=0$ if $V(x,t)=0$, we may impose the weaker condition that $x=0$ if all components of $\nu(x,t)$ vanish. Our proof shows that all components of $\nu[x_2(t)-x_1(t),t]$ vanish identically on $0\leqq t<a$, and the uniqueness follows.

If x has components $(x_1,\cdots,x_n)$, a possible choice of V is $V(x,t) = \sum_{i=1}^{n}|x_i|$, which is easily verified to have the required properties. With this choice of V, the condition (4) becomes

$$\sum_{i=1}^{n}|f_i(x,t)-f_i(y,t)|\leqq\omega[\sum_{i=1}^{n}|x_i-y_i|,t] \tag{11}$$

and Theorem 1 yields Kamke's general uniqueness theorem ([4], p. 139).

Let $\omega(r,t)$ *be a continuous non-negative function defined on* $r\geqq 0$, $0<t<a$. *Suppose the only solution of* (2) *which satisfies* (3) *on* $0\leqq t\leqq\alpha$, *for any* α *in* $0<\alpha<a$, *is the identically zero solution. Let* $f(x,t)$ *be continuous in a region* $0<t<a$, $\sum_{i=1}^{n}x_i(t)<b$ *and satisfy* (11) *there. Then there is at most one solution of* (1) *on* $0\leqq t<a$.

If we take $\omega(r,t)=\phi(r)\lambda(t)$, we obtain Osgood's uniqueness theorem.

If $f(x,t)$ *is continuous in* $0<t<a$, $\sum_{i=1}^{n}|f_i(x,t)|<b$, *and satisfies*

$$\sum_{i=1}^{n}|f_i(x,t)-f_i(y,t)|\leqq\phi(\sum_{i=1}^{n}|x_i-y_i|)\lambda(t),$$

where

$$\int_0 dr/\phi(r)=\infty,\qquad\int_0^a\lambda(t)\,dt<\infty,$$

then there is at most one solution of (1) *on* $0\leqq t<a$.

3. Let $f(x,t)$ be defined and continuous on all of $R^n\times R^1$. As is shown by the example $f(x,t)=1+x^2$ $(n=1)$, there may be solutions to (1) which can not be continued for all t, and thus additional conditions must be imposed on f to ensure the existence of global solutions. The fundamental fact which underlies all the explicit criteria is the following (cf. Wintner [8]):

THEOREM 2. *If* $x(t)$ *is a solution of* (1) *which is defined for some time interval bounded on the right by* t_0, *then either* $\|x(t)\|\to\infty$ *as* $|t|\to t_0$ *or the solution can be extended beyond* t_0.

The proof consists merely in observing that if $\| x(t) \|$ did not go to infinity, then there would exist a sequence t_k such that $t_k \to t_0$ and $x(t_k) \to x_0$, where x_0 is some point in R^n. But the function f will be bounded in any compact neighbourhood N of (x_0, t_0), so that the local existence theorem assures the existence of a solution curve through any point of N, and this solution will be defined for a length of time depending only on the distance to the boundary of N. Thus, applying the local existence theorem to $(x(t_k), t_k)$ for k large enough, we obtain a continuation of $x(t)$ beyond t_0.

An immediate corollary of this theorem is that if T is a mapping of $R^n \times R^1 \to R^j$ with the property that the inverse image of a compact set is compact, then either $\| T[x(t), t] \| \to \infty$ as $t \to t_0$ or $x(t)$ can be continued beyond t_0. In particular, using arguments similar to those in Section 2, we have the following criterion due to Conti [2] (who gives essentially the same proof).

THEOREM 3. *Let* $V(x,t)$ *be a positive real-valued function as in Section 2 such that*

$$V_t(x,t) + V_x \cdot f(x,t) \leqq \omega[V(x,t), t],$$

where ω *has the property that any solution of* (2) *can be continued for all time. Then if the inverse image of a compact set under* V *in* R^n *is compact for all fixed* t*, then the solutions of* (1) *can be continued for all time.*

If we take $V(x,t)$ to be $\| x \|$, we obtain the majorization principle of Wintner [9]. If, in addition, we take $\omega(r,t) = \phi(r)\lambda(t)$, we obtain the following well-known criterion due to Wintner [8].

If $| f(x,t) | \leqq \phi(\| x \|)\lambda(t)$, *where* $\int^{\infty} dr/\phi(r) = \infty$, *then the solutions of* (1) *can be extended for all time.*

The striking analogy between the theorems of Section 2 and the criteria of the present section are easily understood on the basis of Theorem 2. In fact, Theorem 2 says that the solution at infinity is not unique if continuation for all time is not possible. This notion can be made precise by choosing some smooth homeomorphism M of $0 < \| y \| < \infty$ onto itself such that $M(y) \to 0$ for $\| y \| \to \infty$. If we choose M to vanish sufficiently rapidly at infinity, then the right side of the equation

$$z'(s) = -M_y \cdot f \text{ if } z \neq 0, \; z' = 0 \text{ if } z = 0, \tag{12}$$

where $z = M(y)$, $s = -t$, will be continuous for all (z, s). The existence in the large of solutions of (1) is then equivalent to uniqueness at $z=0$ of solutions of (12). If, for example, $n=1$ and $f(x,t)=\phi(|x|)\lambda(t)$, then the Osgood condition goes over into the Wintner condition by a change of variable in the integral.

4. In this section we show that the criterion of Section 2 does not imply convergence of the successive approximations. The well-known example, due to Müller [6], of an initial value problem (1) which has a unique solution but for which the successive approximations do not converge will do this. In fact, there exist V and ω such that Müller's example satisfies the hypotheses of Theorem 1.

Müller's example is the function f $(n=1)$ defined by

$$\begin{aligned}
f(x,t) &= 0, & t &= 0, -\infty < x < +\infty \\
f(x,t) &= 2t, & 0 &< t \leqq 1, -\infty < x < 0 \\
f(x,t) &= 2t - 4x/t, & 0 &< t \leqq 1, 0 \leqq x \leqq t^2 \\
f(x,t) &= -2t, & 0 &< t \leqq 1, t^2 < x < +\infty.
\end{aligned}$$

We choose $V(x,t)=|x|^{\frac{1}{2}}$, and then $V_x(x,t)=\pm\frac{1}{2}|x|^{-\frac{1}{2}}$. It is clear that $|f(x,t)-f(y,t)| \leqq 4t$ and that no smaller bound can be used. The condition (4) becomes

$$\pm\tfrac{1}{2}|x-y|^{-\frac{1}{2}}[f(x,t)-f(y,t)] \leqq \omega(|x-y|^{\frac{1}{2}},t),$$

which is satisfied with $\omega(r,t)=2t/r$. The problem (2), (3), with this choice of ω, has only the trivial solution, and thus, by Theorem 1, the problem (1) for this choice of f has a unique solution.

5. Müller's example, described in Section 4, shows that uniqueness does not imply the convergence of successive approximations. If we start with an equation with non-unique solution, then the successive approximations will trivially converge if we choose a solution as initial curve. The question arises as to whether convergence for an *arbitrary* initial curve is sufficient to imply uniqueness. Here, we provide a counter-example, suggested by Prof. J. Dieudonné and reproduced here with his kind permission after some slight modifications. That is, we shall choose an f such that for arbitrary integrable initial curves $x_0(t)$ with $x_0(0)=0$, the sequence

$$x_j(t)=\int_0^x f[x_{j-1}(s),s]\,ds, \qquad (n=1,2,\cdots) \tag{13}$$

converges, and hence to a solution of (1), and yet (1) has more than one solution.

The most popular example of non-uniqueness, namely $f(x,t) = 2\,|\,x\,|^{\frac{1}{2}}$, has this property. To prove this, we first remark that the procedure (13) is monotone: if $|\,x_0\,| \geqq |\,x_0^*\,|$ for all sufficiently small t, then $|\,x_j\,| \geqq |\,x_j^*\,|$ for such t. Next, we observe that the procedure converges for $x_0(t) = 0$ $[t < a]$, $x_0(t) = k(t - a)^2$ $[t \geqq a]$. In fact,

$$x_j(t) = 0 \ [t < a], \ x_j(t) = k^{1/2^j}(t - a)^2 \ [t \geqq a],$$

so that $x_j(t)$ converges to the solution $x(t) = 0$ $[t < a]$, $x(t) = (t - a)^2$ $[t \geqq a]$.

Now we may assume, iterating several times if necessary, that the initial curve x_0 is non-negative, continuous, and monotone increasing. If $\tau = \operatorname*{g.l.b.}_{x_0(t) > 0} t > 0$, then

$$k_1(t - \tau - \delta)^2 > x_0(t) > k_2(t - \tau + \delta)^2, \tag{14}$$

for any fixed bounded range of $t > \tau, \delta > 0$, and suitably large k_1 and small k_2. Since the procedure (13) is monotone and δ can be made arbitrarily small, (14) implies that $x_j(t)$ converges to the solution $x(t) = 0$ $[t < \tau]$, $x(t) = (t - \tau)^2$ $[t \geqq \tau]$. In fact, it follows that by proper choice of the initial curve $x_0(t)$, the approximations $x_j(t)$ can be made to converge to any solution of (1).

6. In the present section we shall impose an additional condition on V which will imply the convergence of successive approximations. We assume that V has the properties required in Section 2, and also obeys

$$\begin{aligned} &V\Big(\int_{t-h}^{t} [f(x(s),s) - f(y(s),s)]\,ds, t\Big) \\ &\qquad \leqq \int_{t-h}^{t} V_t[x(s) - y(s), s]\,ds + \int_{t-h}^{t} V_x \cdot [f(x(s),s) - f(y(s),s)]\,ds, \end{aligned} \tag{15}$$

for any continuous functions f, x, y.

THEOREM 4. *Let V be as in Section 2, with the additional property* (15). *Suppose the hypotheses of Theorem* 1 *are satisfied with a function $\omega(r,t)$ which is monotone non-decreasing in r for each fixed t. Then the successive approximations* (13) *converge to the solution $x(t)$ of* (1), *in the sense that $V[x(t) - x_j(t), t]$ tends uniformly to zero.*

Proof. It is easy to see that since f is continuous, and hence bounded, the sequence $x_j(t)$ of successive approximations is uniformly bounded and equicontinuous in the Euclidean norm on some interval. It follows that there is a subsequence $x_{j_k}'(t)$ which converges uniformly on this interval (in the Euclidean norm) to a function $x(t)$. Since

$$x_{j_k+1}(t) = \int_0^t f[x_{j_k}(s), s]\,ds,$$

$x_{j_k+1}(t)$ converges uniformly to a function $x^*(t)$. We shall prove

$$V[x_{j+1}(t) - x_j(t), t] \to 0, \tag{16}$$

on this interval, which will imply $x(t) = x^*(t)$, so that $x(t)$ is a solution of (1). Since this solution is unique by Theorem 1, every convergent subsequence converges to $x(t)$, and it follows that the original sequence converges to $x(t)$. Since this sequence is uniformly bounded and equicontinuous, the convergence is uniform in the Euclidean norm, which implies, by the continuity of V, that $V[x(t) - x_j(t), t]$ converges uniformly to zero on some interval.

To prove (16), let $w_j(t) = x_{j+1}(t) - x_j(t)$, and $m(t) = \limsup V[w_j(t), t]$ as $j \to \infty$. Then $m(0) = 0$, and $m(t)$ is continuous, since it is the upper limit of a uniformly bounded equicontinuous sequence of functions. We have

$$\begin{aligned} V[w_{j+1}(t) - w_{j+1}(t-h), t] &= V\Big(\int_{t-h}^t [f(x_{j+1}(s), s) - f(x_j(s), s)]\,ds, t\Big) \\ &\leqq \int_{t-h}^t V_t[x_{j+1}(s) - x_j(s), s]\,ds + \int_{t-h}^t V_x \cdot [f(x_{j+1}(s), s) - f(x_j(s), s)]\,ds, \end{aligned} \tag{17}$$

by (15), and by (4), this is no greater than $\int_{t-h}^t \omega[V(w_j(s), s)]\,ds$. Given any $\delta > 0$, there exists an integer $N(\delta)$, independent of s and j, such that

$$V[w_j(s), s] < m(s) + \delta, \qquad j > N(\delta). \tag{18}$$

This follows from the fact that m is uniformly continuous and w_j is equicontinuous. Since $\omega(r, t)$ is assumed non-decreasing in r, it follows from (18) that

$$\int_{t-h}^t \omega[V(w_j(s), s)]\,ds \leqq \int_{t-h}^t \omega[m(s) + \delta, s]\,ds, \qquad j > N(\delta).$$

Using (17), we obtain

$$V[w_{j+1}(t) - w_{j+1}(t-h), t] \leqq \int_{t-h}^t \omega[m(s) + \delta, s]\,ds, \qquad j > N(\delta). \tag{19}$$

From the definition of $m(t)$ and (19), it is easy to see that

$$m(t) - m(t-h) \leqq \int_{t-h}^t \omega[m(s) + \delta, s]\,ds. \tag{20}$$

Since $\omega(r,t)$ is continuous in r,

$$\omega[m(s)+\delta, s] \to \omega[m(s), s], \qquad \delta \to 0,$$

and this together with (20) yields

$$m(t) - m(t-h) \leqq \int_{t-h}^{t} \omega[m(s), s]\,ds. \tag{21}$$

This implies that $m^*(t) = \limsup_{h\to 0} [m(t) - m(t-h)]/h \leqq \omega[m(t), t]$. The same argument used in the proof of Theorem 1 from (6) on shows that $m(t)$ vanishes identically, which proves the theorem.

The condition that $\omega(r,t)$ be monotone non-decreasing in r can be removed by means of the following lemma.

Lemma. *Let $\omega_1(r,t)$ and $\omega(r,t)$ be two continuous non-negative functions on $0 < t < a$, $r \geqq 0$, such that $\omega_1(r,t) \leqq \omega(r,t)$ on this domain. Suppose that the only solution of (2), (3) on $0 \leqq t \leqq \alpha$, $0 < \alpha < a$, is the identically zero solution. Then the only solution of*

$$r'(t) = \omega_1(r,t), \qquad r(0) = r'(0) = 0, \tag{22}$$

on $0 \leqq t \leqq \alpha$, $0 < \alpha < a$, is the identically zero solution.

Proof. Suppose $m_1(t)$ is a solution of (22) which does not vanish identically, so that there exists σ, $0 < \sigma < a$, such that $m_1(\sigma) > 0$. Through the point $(\sigma, m_1(\sigma))$ there is a solution $m(t)$ of (2) existing on some interval to the left of σ. Since $\omega_1(r,t) \leqq \omega(r,t)$, the proof used to show (7) shows that as far to the left of σ as $m(t)$ exists, it satisfies

$$0 < m(t) \leqq m_1(t). \tag{23}$$

Thus $m(t)$ can be continued to the whole interval $0 < t \leqq \sigma$. It is easy to see that $\lim_{t\to 0} m(t) = 0$, so that we may define $m(0) = 0$. It is also easy to show that $m'(0) = 0$. Thus $m(t)$ is a solution of (2) which satisfies (3). By hypothesis, $m(t)$ must vanish identically on $0 \leqq t \leqq \sigma$, contradicting the choice of $m_1(\sigma)$, and this proves the lemma.

Now, to remove the monotone condition in Theorem 4, we use

$$\omega_1(r,t) = \sup_{V(x-y,t) \leqq r} (V_t(x-y,t) + V_x \cdot [f(x,t) - f(y,t)]) \tag{24}$$

in place of $\omega(r,t)$ if $\omega(r,t)$ is not monotone. It is clear that (24) is monotone in r and satisfies the hypotheses of the lemma. The lemma shows that the hypotheses of Thoerem 4 are satisfied with ω_1 in place of ω, and the conclusion follows.

The use of $V(x,t)=\sum_{i=1}^{n}|x_1|$ in Theorem 4 yields the result of Coddington and Levinson [1]:

Let the hypotheses of Kamke's general uniqueness theorem be satisfied. Then the successive approximations (13) *converge uniformly on some interval to the solution of* (1).

The monotonicity condition imposed in [1] is unnecessary, as we have remarked. The additional condition (15) takes the form

$$(25)\quad \sum_{i=1}^{n}\left|\int_{t-h}^{t}[f_i(x(s),s)-f_i(y(s),s]ds\right| \leqq \int_{t-h}^{t}\sum_{i=1}^{n}|f_i(x(s),s)-f_i(y(s),s)|\,ds$$

in this case, and this condition is obviously satisfied.

THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] E. A. Coddington and N. Levinson, "Uniqueness and the convergence of successive approximations," *Journal of the Indian Mathematical Society*, vol. 16 (1952), pp. 75-81.

[2] R. Conti, "Limitazioni 'in ampiezza' della soluzioni di un sistema di equazioni differenziali e applicazioni," *Bolletino della Unione Matematica Italiana*, ser. 3, vol. 11 (1956), pp. 344-350.

[3] J. Dieudonné, "Sur la convergence des approximations successives," *Bulletin des Sciences Mathématiques*, vol. 69 (1945), pp. 62-72.

[4] E. A. Kamke, *Differentialgleichungen reeller Funktionen*, Leipzig, 1930.

[5] M. A. Krasnosel'skii and S. G. Krein, "Nonlocal existence and uniqueness theorems for differential equations," *Doklady Akademia Nauk SSSR*, vol. 102 (1955), pp. 13-16 (Russian).

[6] M. Müller, "Über das Fundamentaltheorem in der Theorie der gewöhnlichen Differentialgleichungen," *Mathematische Zeitschrift*, vol. 26 (1927), pp. 619-645.

[7] A. Wintner, "On the convergence of successive approximations," *American Journal of Mathematics*, vol. 68 (1946), pp. 13-19.

[8] ———, "The infinities in the non-local existence problem of ordinary differential equations," *ibid.*, vol. 68 (1946), pp. 173-178.

[9] ———, "Ordinary differential equations and Laplace transforms" (Appendix), *ibid.*, vol. 79 (1957), pp. 265-294.

RECIPROCITY AND CORRESPONDENCES.*

By Serge Lang.

To Artin on his 60th birthday

The reciprocity theorem $f((g)) = g((f))$ on a curve arose first in Weil's investigations of Artin's reciprocity law on curves [4]. It has recently been used to deal with various questions of duality, for instance by Igusa [1]. Furthermore, Tate has just given a pairing of certain Galois cohomology groups of abelian varieties [3]. To prove the pairing well defined and bilinear on Jacobians, he used the above theorem.

In this manner, we are therefore led in a natural way to formulate it on abelian varieties, and by pull back on varieties. Aside from its application to the Tate pairing, we get an obvious complement to Kummer theory arising from the theory of divisorial correspondences.

1. Notation. Let U, V be two complete varieties, non-singular in codimension 1. This insures that a divisor which is linearly equivalent to 0 has this property over a given field of rationality and, also, that such a divisor determines uniquely the function of which it is the divisor, up to a multiplicative constant.

A cycle of codimension 1 on a variety will always be called a divisor. A cycle of dimension 0 will be called simply a cycle. Let $\mathfrak{a} = \sum n_i(P_i)$ be a cycle on U. Let ϕ be a function on U such that ϕ is defined at every point of $\mathfrak{a}$ and does not take on the value 0. Then we define

$$\phi(\mathfrak{a}) = \prod \phi(P_i)^{n_i}.$$

If $\mathfrak{a}$ is of degree 0, and ψ is a function such that $\psi = c\phi$ where c is constant, then $\psi(\mathfrak{a}) = \phi(\mathfrak{a})$.

Let D be a divisor on the product $U \times V$. Let $\mathfrak{a}$, $\mathfrak{b}$ be two cycles of degree 0 on U and V respectively. Assume that $D(\mathfrak{a})$ is defined and that it is the divisor of a function f on V. If in addition $f(\mathfrak{b})$ is defined, then we put $D(\mathfrak{a}, \mathfrak{b}) = f(\mathfrak{b})$ and say that $D(\mathfrak{a}, \mathfrak{b})$ is defined.

Suppose that, for every point P in $\mathfrak{a}$ and every point Q in $\mathfrak{b}$, the point

---

* Received January 6, 1958.

(P,Q) does not lie in the support of D (or as we shall say more briefly, in D). Then first, $D(\mathfrak{a})$ is defined, and Q does not lie in the divisor of the function f. Hence $f(Q)$ is defined and not equal to 0, and consequently, $D(\mathfrak{a},\mathfrak{b})$ is defined. This sufficient condition will be used constantly in the sequel.

2. The theorem of the square. The proof of our main reciprocity theorem (Theorem 4) is based on the theorem of the square, which runs as follows.

Let U, V, W be three varieties and assume that W is complete and non-singular in codimension 1. *Let D be a divisor on $U \times V \times W$, and let u_i, v_j $(i,j=0,1)$ be simple points of U, V respectively, such that $D(u_i,v_j)$ is defined. Then $\sum_{i,j}(-1)^{i+j}D(u_i,v_j)$ is linearly equivalent to* 0 *on W.*

This is an immediate consequence of the existence of the Picard variety for W. Indeed, if a, b are two simple points of U, V respectively, such that $D(a,b)$ is defined, then for u, v generic we have a rational map

$$(u,v)\rightarrow \mathrm{Cl}[D(u,v)-D(a,b)]$$

of $U\times V$ into the Picard variety of W. (As usual, Cl denotes the point associated with the linear equivalent class on the Picard variety.) A rational map of a product into an abelian variety splits into a sum of mappings of the factors. It is then clear that in our alternating sum, the constants will cancel, and the alternating sum will map on 0 in the Picard variety. It is therefore linearly equivalent to 0.

Conversely, as Weil has shown, one can give a direct proof for the theorem of the square, and one can base on it the construction of the Picard variety. For this as well as all further information concerning abelian varieties, the reader is referred to [2].

3. The theorem of the hypercube. In order to avoid too many indices, we restrict ourselves to four-fold products, which will be all that is needed for the applications we have in mind to abelian varieties. The notation we now describe will remain fixed throughout this section.

Let U, V, W, T be four varieties, defined over a field k. We assume them complete and non-singular in codimension 1.

Let D be a divisor on the product $U\times V\times W\times T$, rational over k. Let i, j, k, l range over 0 and 1, and take two copies of each one of our four varieties, U_i, V_j, W_k, T_l. On the double product

$$U_0 \times U_1 \times V_0 \times V_1 \times W_0 \times W_1 \times T_0 \times T_1 = U^{(2)} \times V^{(2)} \times W^{(2)} \times T^{(2)},$$

consider the divisor D_{ijkl} consisting of D on the partial product

$$U_i \times V_j \times W_k \times T_l$$

taken with the full varieties on the others. (In other words, it is the inverse image of D under the projection of the eight-fold product to the four-fold product.) We can take a coboundary of D, by setting

$$E = \sum (-1)^{i+j+k+l} D_{ijkl},$$

and observe that this formula could have been generalized to arbitrary products.

Let
$$P = (u_0, u_1, v_0, v_1) \quad \text{and} \quad Q = (w_0, w_1, t_0, t_1)$$

be two independent generic points of $U^{(2)} \times V^{(2)}$ and $W^{(2)} \times T^{(2)}$ over k. By the theorem of the square, there exists a function f_P on $W \times T$, defined over $k(P)$, and a function g_Q on $U \times V$, defined over $k(Q)$ such that

$$(1) \qquad (f_P) = \sum (-1)^{i+j} D(u_i, v_j) \quad \text{and} \quad (g_Q) = \sum (-1)^{k+l}\, {}^tD(w_k, t_l).$$

Furthermore, it is obvious from the definitions that we have

$$(2) \qquad E(P) = \sum (-1)^{k+l} (f_P)_{kl} = \sum_{i,j,k,l} (-1)^{i+j+k+l} D(u_i, v_j)_{kl}$$

$$(3) \qquad {}^tE(Q) = \sum (-1)^{i+j} (g_Q)_{ij} = \sum_{i,j,k,l} (-1)^{i+j+k+l}\, {}^tD(w_k, t_l)_{ij}.$$

All further reciprocity theorems derived from the correspondence D between $U \times V$ and $W \times T$ arise from the symmetry of our divisor E.

THEOREM 1. *The divisor E above is linearly equivalent to* 0.

Proof. There exists a function f^* on $U^{(2)} \times V^{(2)} \times W \times T$ defined over k such that

$$f^*(P, w, t) = f_P(w, t),$$

and we have

$$P \times (f_P) = (f^*) \cdot (P \times W \times T).$$

There exists a function F on the eight-fold product such that

$$(4) \qquad F(u_0, u_1, v_0, v_1, w_0, w_1, t_0, t_1) = \prod f^*(P, w_k, t_l)^{(-1)^{k+l}},$$

and from the definitions, we see that $(F)(P) = E(P)$. Hence (F) and E differ by a divisor which is degenerate on $U^{(2)} \times V^{(2)}$. Inducing (F) and E on the variety $U^{(2)} \times V^{(2)} \times W^{(2)} \times \Delta_T$, we obtain 0. Hence the degenerate component is equal to 0, and we have $(F) = E$, as desired.

Note that the function F such that $E = (F)$ is defined at the point obtained by setting $t_0 = t_1$, and takes the value 1. This gives us a way of normalizing it, since two functions representing E differ by a multiplicative constant.

On the other hand, from the symmetry of F, we see that if we go from right to left in the correspondence given by D, then we obtain the following reciprocity formula, from (4).

THEOREM 2. *Let F be a function on the eight-fold product, defined over k, such that $E = (F)$, and normalized as above. Then*

$$F(P, Q) = \prod f_P(w_k, t_l)^{(-1)^{k+l}} = \prod g_Q(u_i, v_j)^{(-1)^{i+j}}.$$

As usual, such a formula at generic points has its counterpart for special points.

THEOREM 3. *Let (u_0', u_1', v_0', v_1') and (w_0', w_1', t_0', t_1') be two simple points of $U^{(2)} \times V^{(2)}$ and $W^{(2)} \times T^{(2)}$ respectively. Put*

$$\mathfrak{a} = \sum (-1)^{i+j}(u_i', v_j') \qquad \mathfrak{b} = \sum (-1)^{k+l}(w_k', t_l').$$

Assume that none of the points (u_i', v_j', w_k', t_l') lies in the support of D. Then $D(\mathfrak{a}, \mathfrak{b}) = {}^tD(\mathfrak{b}, \mathfrak{a})$.

Proof. It is immediate from our hypothesis that (P', Q') does not lie in $(F) = E$, and hence $F(P', Q')$ is defined. Our equality is now obvious.

4. Application to abelian varieties.

Let A, B be two abelian varieties defined over k, and let D be a divisor on $A \times B$, rational over k. Let $\mathfrak{a}$ be a cycle on A of degree 0, such that $D(\mathfrak{a})$ is defined. If $\mathfrak{a}$ is in the kernel of Albanese, i.e., if $S(\mathfrak{a}) = 0$, then $D(\mathfrak{a})$ is linearly equivalent to 0 on B, say $D(\mathfrak{a}) = (f)$. If now $\mathfrak{b}$ is a cycle of degree 0 on B, also in the kernel of Albanese on B, such that no point of $\mathfrak{a} \times \mathfrak{b}$ is contained in D, then we may form symmetrically either $D(\mathfrak{a}, \mathfrak{b})$ or ${}^tD(\mathfrak{b}, \mathfrak{a})$.

THEOREM 4. *Let A, B be two abelian varieties. Let D be a divisor on $A \times B$. Let $\mathfrak{a}$, $\mathfrak{b}$ be cycles on A, B respectively, of degree 0, such that $S(\mathfrak{a}) = 0$ and $S(\mathfrak{b}) = 0$. Assume no point of $\mathfrak{a} \times \mathfrak{b}$ is contained in D. Then $D(\mathfrak{a}, \mathfrak{b})$ and ${}^tD(\mathfrak{b}, \mathfrak{a})$ are defined, and they are equal.*

Proof. Suppose first that D is the divisor of a function ϕ on $A \times B$. Our hypotheses imply that ϕ is defined at every point of $\mathfrak{a} \times \mathfrak{b}$, and our theorem simply asserts $\phi(\mathfrak{a}, \mathfrak{b}) = \phi(\mathfrak{a}, \mathfrak{b})$. Taking into account an obvious linearity, this remark allows us to change D by suitable linear equivalence.

We shall reduce our theorem to the case where $\mathfrak{a}$ and $\mathfrak{b}$ consist of four points each. This will then allow us to use Theorem 3.

Suppose that $\mathfrak{a}$ is written

$$\mathfrak{a} = (a_1) - (a_1') + (a_2) - (a_2') + \cdots + (a_n) - (a_n').$$

Let x be any point of A. We can write

$$\begin{aligned}\mathfrak{a} = {} & (a_1) - (a_1') + (x) - (x + a_1 - a_1') \\ & + (a_2) - (a_2') + (x + a_1 - a_1') - (x + a_2 - a_2' + a_1 - a_1') + \cdots,\end{aligned}$$

so that we correct each successive step to cancel the preceding term. We must come back at the end with $-(x)$ using the fact that $S(\mathfrak{a}) = 0$. Thus our cycle can be written as a sum of cycles of degree 0, in the kernel of Albanese, and consisting of four points.

From the theory of linear equivalence, one knows that it is possible to find a function ϕ on $A \times B$ such that none of the points of a given finite set of points on $A \times B$ lies in the support of $D + (\phi)$. (We reproduce a proof of this fact in an appendix.) We apply this to the product of the set of points entering in the expression of $\mathfrak{a}$ obtained above, with a similar set for $\mathfrak{b}$. In view of our previous remark, and of an obvious linearity when all necessary expressions are defined, we see that it indeed suffices to prove our theorem when $\mathfrak{a}$ and $\mathfrak{b}$ consist of four points.

Let us therefore write

$$\mathfrak{a} = (a_0) - (a_1) + (a_2) - (a_3),$$

$$\mathfrak{b} = (b_0) - (b_1) + (b_2) - (b_3).$$

Let $\lambda_A : A \times A \rightarrow A$ be the modified law of composition, such that $\lambda_A(u, v) = u - v$, and let $\lambda = (\lambda_A, \lambda_B)$. Let $D^* = \lambda^{-1}(D)$. It is a divisor on the product $A \times A \times B \times B$. Let u be a generic point of A, and let

$$u_0' = u + a_0, \quad u_1' = u + a_3, \quad v_0' = u, \quad v_1' = u + a_0 - a_1.$$

Do a similar construction for the points of $\mathfrak{b}$, to obtain points w_k' and t_l'. By hypothesis, no point of $\mathfrak{a} \times \mathfrak{b}$ lies in D, and hence none of the points (u_i', v_j', w_k', t_l') lies in D^*. We have

$$\sum (-1)^{i+j} D^*(u_i', v_j') = \lambda_B^{-1}[\sum (-1)^{\nu} D(a_\nu)].$$

If we put $\mathfrak{a}^* = \sum (-1)^{i+j} (u_i', v_j')$, we can also write

$$D^*(\mathfrak{a}^*) = \lambda_B^{-1} D(\mathfrak{a}).$$

This comes from commutativity in the diagram

$$\begin{tikzcd}(x,y)\times B\times B \arrow[r, "\lambda"] \arrow[d, "\mathrm{inj}"'] & (x-y)\times B \arrow[d, "\mathrm{inj}"] \\ A\times A\times B\times B \arrow[r, "\lambda"] & A\times B\end{tikzcd}$$

where inj is the injection, together with the formalism of the inverse mappings of cycles applied to the divisor D (cf. the appendix of [2]).

Similarly, we have a cycle $\mathfrak{b}^*$ such that

$$^tD^*(\mathfrak{b}^*)=\lambda_A^{-1}\,{}^tD(\mathfrak{b}).$$

If $(f)=D(\mathfrak{a})$, we have a function $f^*=f\lambda_B$, and if $(g)={}^tD(\mathfrak{b})$ we have a function $g^*=g\lambda_A$. Then

$$(f^*)=\lambda_B^{-1}(f)=\lambda_B^{-1}D(\mathfrak{a}) \quad\text{and}\quad (g^*)=\lambda_A^{-1}(g)=\lambda_A^{-1}\,{}^tD(\mathfrak{b}).$$

By Theorem 3, $f^*(\mathfrak{b}^*)=g^*(\mathfrak{a}^*)$ and hence clearly, $f(\mathfrak{b})=g(\mathfrak{a})$. This proves our theorem.

By pull back, we now obtain the following result for varieties.

THEOREM 5. *Let V, W be two complete varieties, non-singular in codimension* 1, *and such that any finite set of points on them can be represented on an affine open subset. Let $\phi: V\to A$ and $\psi: W\to B$ be two canonical maps into their Albanese varieties. Let $\mathfrak{a}$, $\mathfrak{b}$ be two cycles on V, W respectively, of degree* 0, *and in the kernel of Albanese. Let D be a divisor on $V\times W$ such that no point of $\mathfrak{a}\times\mathfrak{b}$ lies in D. Then $D(\mathfrak{a},\mathfrak{b})$ and $^tD(\mathfrak{b},\mathfrak{a})$ are defined and they are equal.*

Proof. If the theorem is true for one divisor D in a correspondence class on $V\times W$, then it is true for every divisor in that class not containing any point of $\mathfrak{a}\times\mathfrak{b}$. This is first checked for linear equivalence, and then for degenerate divisors. A representative divisor in a correspondence class can always be obtained as an inverse image of a divisor on $A\times B$, and our result is now an immediate consequence of the formalism of inverse mappings of cycles, applicable in the present case to the commutative diagram

$$\begin{tikzcd}\mathfrak{a}\times W \arrow[r, "(\phi,\psi)"] \arrow[d, "\mathrm{inj}"'] & \phi(\mathfrak{a})\times B \arrow[d, "\mathrm{inj}"] \\ V\times W \arrow[r, "(\phi,\psi)"] & A\times B.\end{tikzcd}$$

COROLLARY. *Let C be a complete non-singular curve, and let f, g be* *two functions on C whose divisors have no point in common. Then* $f((g)) = g((f))$.

Proof. Take the diagonal on $C \times C$. Our hypothesis means that no point of $(f) \times (g)$ lies in it, and we can apply the theorem.

5. The Tate pairing. Let A, B be two abelian varieites, defined over the field k. Let D be a divisor on $A \times B$, rational over k, and let K be a finite Galois extension of k, with group G. If M is a G-module, we have cohomology groups $H^r(G, M)$. Since G will be fixed throughout, we shall also write $H^r(M)$.

The groups A_K and B_K of rational points of A and B respectively, in K are such G-modules. We wish to define a pairing of $H^1(A_K)$ and B_k into $H^2(K^*)$, where K^* is the multiplicative group of K. This is done as follows.

Let (a_σ) be a 1-cocycle in A_K and let $b \in B_k$. Denote by $Z_0(V, K)$ the group of zero cycles on a variety V, of degree 0, rational over K. Let $\mathfrak{a}_\sigma$ be in $Z_0(A, K)$, and such that $S(\mathfrak{a}_\sigma) = a_\sigma$. We can form the coboundary

$$\mathfrak{a} = (\delta\mathfrak{a})_{\sigma,\tau} = \sigma\mathfrak{a}_\tau - \mathfrak{a}_{\sigma\tau} + \mathfrak{a}_\sigma,$$

and we have $S(\mathfrak{a}) = 0$. Select $\mathfrak{b}$ in $Z_0(B, k)$ such that $S(\mathfrak{b}) = b$. We put

$$\alpha_{\sigma,\tau} = D(\mathfrak{a}, \mathfrak{b})$$

after changing D by the divisor of a function over k if necessary, to make this expression defined.

It is clear that $(\alpha_{\sigma,\tau})$ is a 2-cocycle of G in K^*. We contend that its cohomology class depends only on the linear equivalence class of D, and, in fact, on its correspondence class, and that the pairing

$$[(a_\sigma), b] \to (\alpha_{\sigma,\tau})$$

induces a well defined bilinear map of $H^1(A_K)$ and B_k into $H^2(K^*)$. In addition, if an element of B_k is a trace of an element of B_k, it is orthogonal to $H^1(A_K)$ so that we may replace B_k by $H^0(B_K)$. This will be proved in the following sequence of assertions.

a.) If D and D' differ by a trivial divisor, of type $X \times B + A \times Y + (\phi)$, and if $\alpha_{\sigma,\tau}$ and $\alpha_{\sigma,\tau}'$ are obtained, respectively, from D and D' as above, then they are cohomologous.

Proof. To begin with, we must insure that if D and D' differ by the divisor of a function (ϕ), $\phi \in k(A \times B)$, then our cocycles are cohomologous.

Indeed, $\alpha_{\sigma,\tau}$ and $\alpha_{\sigma,\tau}'$ differ by the coboundary of $\phi(\mathfrak{a}_\sigma, \mathfrak{b})$. The rest is now trivially verified.

b.) If $\mathfrak{a}_\sigma$ is changed by a cycle of type $\mathfrak{a}_\sigma' + (\sigma - 1)\mathfrak{c}$ with $\mathfrak{a}_\sigma' \in Z_0(A, K)$ and $S(\mathfrak{a}_\sigma') = 0$, then $\alpha_{\sigma,\tau}$ changes by a coboundary.

Proof. In fact, that coboundary is that of $D(\mathfrak{a}_\sigma', \mathfrak{b})$.

c.) If we change $\mathfrak{b}$ by a cycle $\mathfrak{c} \in Z_0(B, k)$ such that $S(\mathfrak{c}) = 0$, then $\alpha_{\sigma,\tau}$ changes by a coboundary.

Proof. Using the reciprocity theorem, one sees that the coboundary is that of ${}^tD(\mathfrak{c}, \mathfrak{a}_\sigma)$.

The above statements show that our pairing is well defined. That it is bilinear now follows from the bilinearity of $D(\mathfrak{a}, \mathfrak{b})$.

d.) If b is a trace, $b = \sum \rho b'$, then $\alpha_{\sigma,\tau}$ is a coboundary.

Proof. We can choose $\mathfrak{b} = \sum (\rho' b') - n(0)$. Then the coboundary is that of

$$c_\sigma = \prod_\rho f_{\sigma,\rho}(\sigma\rho b')/f_{\sigma,\rho}(0).$$

6. Kummer theory. Let A, B be two abelian varieties and D a divisor on the product. Let $\mathfrak{a}$, $\mathfrak{b}$ be two cycles on A and B respectively, of degree 0. We write $\mathfrak{a} \sim 0$ if $S(\mathfrak{a}) = 0$. Assume that there is an integer n such that $n\mathfrak{a} \sim 0$ and $n\mathfrak{b} \sim 0$. Let D_1 be linearly equivalent to D, and such that no point of $\mathfrak{a} \times \mathfrak{b}$ lies in D_1. Then one verifies immediately that ${}^tD_1(n\mathfrak{b}, \mathfrak{a})/D_1(n\mathfrak{a}, \mathfrak{b})$ is an n-th root of unity which is independent of the auxiliary divisor D_1 selected in the linear equivalence class of D. We shall denote it by $\varepsilon_{n,D}(\mathfrak{a}, \mathfrak{b})$. Furthermore, if $\mathfrak{a}_1 \sim \mathfrak{a}$ and $\mathfrak{b}_1 \sim \mathfrak{b}$, then $\varepsilon_{n,D}(\mathfrak{a}, \mathfrak{b}) = \varepsilon_{n,D}(\mathfrak{a}_1, \mathfrak{b}_1)$. Thus our root of unity defines a bilinear pairing of the points of order n on A and B respectively. If $a = S(\mathfrak{a})$ and $b = S(\mathfrak{b})$, so that $na = 0$ and $nb = 0$, we can also write $\varepsilon_{n,D}(a, b)$ instead of $\varepsilon_{n,D}(\mathfrak{a}, \mathfrak{b})$. Note finally that it depends only on the correspondence class of D.

On the other hand, we can obviously generalize the root of unity defined by Weil which is usually denoted by $e_n(a, b)$ in the special case of divisors on an abelian variety, i.e., when $B = \hat{A}$ and D is a Poincaré divisor. Namely, it is clear that $(n\delta)^{-1}\,{}^tD(\mathfrak{b})$ is linearly equivalent to 0 on A if $n\mathfrak{b} \sim 0$. Say $(\omega) = (n\delta)^{-1}\,{}^tD(\mathfrak{b})$. Let u be a generic point of A. Then $\omega(u + a)/\omega(u)$ is by definition, the n-th root of unity $e_{n,D}(a, b)$. (See [2], Ch. 7.)

THEOREM 6. *Let D be a divisor on a product of abelian varieties $A \times B$.*

Let $\mathfrak{a}$, $\mathfrak{b}$ *be two cycles on* A *and* B *respectively, of degree* 0, *such that* $n\mathfrak{a} \sim 0$ *and* $n\mathfrak{b} \sim 0$. *Let* $a = S(\mathfrak{a})$ *and* $b = S(\mathfrak{b})$. *Then* $\varepsilon_{n,D}(a, b) = e_{n,D}(a, b)$.

Proof. Consider the rational map $n\delta : A \rightarrow A$ followed by the divisorial correspondence D on $A \times B$. Just as in the appendix of [2], we form the composed divisor on $A \times B$, which we denote by $E = D \circ (n\delta)$. Then it is obvious that E and nD are in the same correspondence class on $A \times B$, and thus that

$$E = nD + (F) + X \times B + A \times Y$$

for some function F on $A \times B$, and divisors X on A and Y on B. Let k be a field of rationality for D, E, F, X and Y, and let u, w be independent generic points of A, B over k. We put

$$\mathfrak{a} = (u + a) - (u) \quad \text{and} \quad \mathfrak{b} = (w + b) - (w).$$

Then

$$e_{n,D}(\mathfrak{a}, \mathfrak{b}) = {}^tE(\mathfrak{b}, \mathfrak{a}) = {}^tD(n\mathfrak{b}, \mathfrak{a})F(\mathfrak{a}, \mathfrak{b}).$$

On the other hand, $E(\mathfrak{a}) = D(nu + na) - D(nu) = 0$, and hence $E(\mathfrak{a}, \mathfrak{b}) = 1$. Thus $D(n\mathfrak{a}, \mathfrak{b})^{-1} = F(\mathfrak{a}, \mathfrak{b})$. This proves our theorem.

One should observe that, just as we proved Theorem 5 for arbitrary varieties, we can generalize our root of unity to arbitrary varieties by pull back. The details are obvious and are left to the reader.

Appendix.

From the theory of linear equivalence, one knows that, given two cycles on a projective non-singular variety, it is possible to move one of them by linear equivalence so that the intersection is defined. Samuel has pointed out to me that this can be done rationally over a given field of rationality for all objects involved (at least over an infinite field). We need the result here only for divisors, and I shall reproduce below a proof due to Chevalley. We first deal with the local problem.

THEOREM. *Let* V *be an affine variety defined over a field* k. *Let* D *be a divisor on* V, *rational over* k. *Let* S *be a finite set of simple points of* V. *Then there exists a function* ϕ *on* V, *defined over* k, *such that no point of* S *lies in the support of* $D + (\phi)$.

Proof. We may obviously assume that D is positive and, in fact, a prime rational cycle. Furthermore, we may assume that the points of S are algebraic over k, because D contains the specializations over k of all of its points.

Let $R = k[v]$ be a coordinate ring for V over k and let I be the ideal of R consisting of those functions $f \in R$ such that $(f) \geqq D$. This ideal has a finite basis, $I = (f_1, \cdots, f_n)$. Let $\mathfrak{p}$ be a maximal ideal of R, and $\mathfrak{o} = R_{\mathfrak{p}}$ its local ring with maximal ideal $\mathfrak{m}$. We assume that $\mathfrak{p}$ belongs to a simple point, so that $\mathfrak{o}$ is a unique factorization domain. Then there is a function t in $\mathfrak{o}$ which represents D locally at $\mathfrak{p}$. We can write $t = \sum a_i f_i$ with $a_i \in \mathfrak{o}$. I contend that if $b_i \in \mathfrak{o}$ is such that $b_i \equiv a_i \pmod{\mathfrak{m}}$ then $\sum b_i f_i$ differs from t by a unit in $\mathfrak{o}$. Indeed,

$$\sum b_i f_i = \sum (b_i - a_i) f_i + t.$$

Since $(f_i) \geqq D$, we can write $f_i = t g_i$ with $g_i \in \mathfrak{o}$. Hence $\sum b_i f_i \in t[1 + \mathfrak{m}]$, thereby proving our contention.

Now let $\mathfrak{p}_j$ be a finite number of maximal ideals of R, belonging to simple points. Let $\mathfrak{o}_j = \mathrm{R}_{\mathfrak{p}_j}$ be their local rings with maximal ideals $\mathfrak{m}_j$. Given elements x_j in $\mathfrak{o}_j$. it is possible to find $x \in R$ such that $x \equiv x_j \pmod{\mathfrak{m}_j}$, by the well known Chinese remainder theorem, applicable since $\mathfrak{p}_j + \mathfrak{p}_{j'} = R$ for $j \neq j'$. We now see that it suffices to approximate at each $\mathfrak{o}_j$ by an element of R, the coefficients of an element t, representing D at $\mathfrak{o}_j$ in terms of the f_i. This proves our theorem.

If we wish to apply the local result to an abstract variety V, then we must assume that the given finite set of points (algebraic over k) can be represented on an affine k-open subset of V. This is the case on a projective variety, although, if the ground field is finite, we may have to change the projective embedding (for instance, by finding first a hypersurface section of V which does not pass through any of the given points, and then dehomogenizing V at this hypersurface, in the projective embedding in which this hypersurface becomes a hyperplane).

PARIS.

REFERENCES.

[1] J. Igusa, "Fibre systems of Jacobian varieties, II," *American Journal of Mathematics*, vol. 78 (1956), pp. 745-760.

[2] S. Lang, *Abelian varieties*, Interscience Publishers, New York, 1958.

[3] J. Tate, "Galois cohomology of Abelian varieties over p-adic fields," to appear.

[4] A. Weil, "Sur les fonctions algébriques à corps de constantes fini," *Comptes Rendus de l'Académie des Sciences*, vol. 210 (1940), pp. 592-594.

SPHERICAL FUNCTIONS OVER $\mathfrak{P}$-ADIC FIELDS, I.*

By F. I. Mautner.

1. Introduction and preliminaries. Let Ω be a field which is complete under a given discrete real valued valuation. For every element a of Ω, the order of a is defined and denoted by $\operatorname{ord}(a)$. If $a \neq 0$, then $\operatorname{ord}(a)$ is a rational integer and $a \rightarrow \operatorname{ord}(a)$ is a homomorphism of the multiplicative group $\Omega^{\times}$ of Ω onto the additive group of rational integers; if $a = 0$, we put $\operatorname{ord}(0) = +\infty$. Let $\mathfrak{O}$ be the valuation ring of Ω, i. e., the set of elements a of Ω for which $\operatorname{ord}(a) \geqq 0$, and $\mathfrak{P}$ the unique maximal ideal of $\mathfrak{O}$ defined by $\operatorname{ord}(a) > 0$. The ideal $\mathfrak{P}$ is principal. Let τ be a generator of $\mathfrak{P}$:

$$(1.1) \qquad \mathfrak{P} = (\tau) = \tau\mathfrak{O}, \quad \operatorname{ord}(\tau) = 1.$$

Let $\mathfrak{U}$ be the group of units of the ring $\mathfrak{O}$; this is the set of elements of order zero. Every element $a \neq 0$ of Ω can be written uniquely in the form

$$(1.2) \qquad a = \tau^{n}u, \text{ where } n = \operatorname{ord}(a) \text{ and } u \in \mathfrak{U},$$

so that $\Omega^{\times}$ is the direct product of $\{\tau^{n}\}$ and $\mathfrak{U}$. We shall assume throughout that the residue class field $\mathfrak{O}/\mathfrak{P}$ is finite:

$$(1.3) \qquad q = \mathfrak{N}\mathfrak{P} = \text{number of elements of } \mathfrak{O}/\mathfrak{P} < \infty.$$

We normalize the valuation $|\ |$ on Ω by putting

$$(1.4) \qquad |a| = (\mathfrak{N}\mathfrak{P})^{-\operatorname{ord}(a)} = q^{-\operatorname{ord}(a)}.$$

With $|a - b|$ as distance, Ω is a metric space; it is well known and readily verified that with the topology defined by this metric, Ω is a locally compact topological field, $\mathfrak{O}$ a compact open subring of Ω and each ideal $\mathfrak{P}^{n}$ compact and open. The ideals $\mathfrak{P}^{n}$ $(n = 1, 2, 3, \cdots)$ form a base for the neighborhoods of 0 in Ω, so that Ω is totally disconnected.

The additive group Ω^{+} of Ω being a locally compact topological group, there exists a Haar-measure on it, which we denote by μ. One has

$$(1.5) \qquad d\mu(x + a) = d\mu(x), \qquad d\mu(ax) = |a|\, d\mu(x).$$

---

* Received November 22, 1957.

The first of these two equations expresses merely the invariance of the Haar-measure μ on Ω^+, while the second equation in (1.5) is easily verified using the uniqueness of Haar-measure and the normalization (1.4) of the valuation.

We shall study, in this paper, certain function spaces on the group $G = PG(2, \Omega)$ of fractional linear transformations over Ω. Let $\mathfrak{G}$ be the group $GL(2, \Omega)$ of all non-singular 2×2 matrices with coefficients in Ω and $\mathfrak{Z}$ the center of $\mathfrak{G}$, i.e., the set of scalar matrices $\neq 0$. Both $\mathfrak{G}$ and G are locally compact topological groups, and G is topologically isomorphic to $\mathfrak{G}/\mathfrak{Z}$. We denote the natural homomorphism of $\mathfrak{G}$ onto G by $\mathfrak{G} \to G$.

$$G \cong \mathfrak{G}/\mathfrak{Z}; \qquad \mathfrak{G} \to G. \tag{1.6}$$

Let $\mathfrak{K}$ be the group $GL(2, \mathfrak{O})$ of all 2×2 matrices with coefficients in $\mathfrak{O}$ and determinant in $\mathfrak{U}$. Clearly $\mathfrak{K}$ is a compact open subgroup of $\mathfrak{G}$. Let K be the image of $\mathfrak{K}$ under the natural homomorphism of $\mathfrak{G}$ onto G, so that K is an open and compact subgroup of G.

Definition 1.1. Let S be the class of all complex-valued functions $f(g)$ on G which satisfy

$$f(kgk') = f(g) \text{ for all } g \in G,\ k \text{ and } k' \in K. \tag{1.7}$$

We shall call S the space of spherical functions.

For any positive real number ρ, let $\mathfrak{L}^\rho = \mathfrak{L}^\rho(G)$ be the space of equivalence classes of complex valued Haar-measurable functions $f(g)$ on G whose ρ-th power is Lebesgue-integrable with respect to Haar-measure on G. We put $S^\rho = S \cap \mathfrak{L}^\rho$; in particular, S^1 is a closed subalgebra of $\mathfrak{L}^1$, which will be seen to be commutative. We shall study the spaces S^ρ for $\rho = 1$ or 2 and also the algebra S^0 of all spherical functions $f(g)$ which are of compact support on G.

We obtain an explicit characterization of S^0 by showing that, under the Fourier-transform on G, the algebra S^0 is mapped isomorphically onto the algebra of all even Fourier polynomials and the isomorphism is given explicitly. As far as S^1 is concerned, the situation is analogous to known properties of spherical functions on non-compact semi-simple Lie groups. In particular, it is again true that the Fourier transform of any function in S^1 is a function $F(s)$, regular analytic in the strip $0 < Rs < 1$ and satisfying the functional equation $F(s) = F(1-s)$. We determine all maximal ideals of S^1, showing that they correspond to points in the strip $0 \leqq Rs \leqq 1$. For this purpose, it is useful to compute the elementary spherical functions explicitly. This is done in § 7; it seems remarkable that they are elementary functions (in fact rational functions of q^s). Thus the situation is in this respect more analgous to that of complex semi-simple Lie groups than to the real case.

The results of this paper will be applied elsewhere to the analytic theory of quadratic forms, where it will be shown how they can be used to establish identities between certain of C. L. Siegel's representation functions of quadratic forms and to obtain functions of q^s associated with quadratic forms whose zeros are all on the line $Rs = \frac{1}{2}$ or on the intervals $s + 2\pi in/\log q$ real, $0 < Rs < 1$, also, functions of s whose zeros lie on the line $Rs = \frac{1}{2}$ or on the real interval $0 < s < 1$. These functions can be developed into Dirichlet series absolutely convergent for $Rs > 1$, have a functional equation $(s \rightarrow 1 - s)$ and an analogue of the Euler product; they are different from A. Selberg's generating functions for the order of magnitude of the norms of the primitive elements in discontinuous groups of motion of the hyperbolic plane. Indeed, the coefficients in the Dirichlet series are given in terms of Siegel's representation functions $A(\mathfrak{S}, \mathfrak{T})$ and $\alpha_p(\mathfrak{S}, \mathfrak{T})$ of quadratic forms.

2. The groups $GL(2, \boldsymbol{\Omega})$ and $PGL(2, \boldsymbol{\Omega})$. We put on the group $\mathcal{G} = GL(2, \Omega)$ the topology which it inherits as a subset of the four-dimensional locally compact topological vector space of all 2×2 matrices over Ω (the latter, of course, with the Cartesian product topology of $\Omega \times \cdots \times \Omega$). Clearly $\mathcal{G}$ is a locally compact topological group and $\mathcal{K} = GL(2, \mathfrak{O})$, a compact and open subgroup of $\mathcal{G}$. Hence the factor space $\mathcal{G}/\mathcal{K}$ is discrete in its natural topology.

Using elementary divisors, one sees that every element g of $\mathcal{G}$ can be written in the form

$$g = k_1 \begin{pmatrix} \tau^m & 0 \\ 0 & \tau^n \end{pmatrix} k_2, k_j \in \mathcal{K}. \tag{2.1}$$

To this, we apply the natural homomorphism $\mathcal{G} \rightarrow G$ of $\mathcal{G}$ onto G, whose kernel is $\mathcal{Z}$ (see (1.6) above) and note that there exists an element c of $\mathcal{Z}$ such that $c \begin{pmatrix} \tau^m & 0 \\ 0 & \tau^n \end{pmatrix} = \begin{pmatrix} \tau^{m-n} & 0 \\ 0 & 1 \end{pmatrix}$. Let

$$y = \text{image in } G \text{ of } \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix} \text{ under } \mathcal{G} \rightarrow G. \tag{2.2}$$

We conclude that every element g of G can be written in the form

$$g = k_1 y^n k_2, \qquad k_j \in K, \tag{2.3}$$

since K was defined to be the image of $\mathcal{K}$ under $\mathcal{G} \rightarrow G$.

Now $Ky^mK=Ky^nK$ *is equivalent to* $\mathfrak{K}\begin{pmatrix}\tau^m & 0\\ 0 & 1\end{pmatrix}\mathfrak{K}=\mathfrak{Z}\mathfrak{K}\begin{pmatrix}\tau^n & 0\\ 0 & 1\end{pmatrix}\mathfrak{K}$. Hence

$$\begin{pmatrix}0 & u^{\perp}\\ 0 & 1\end{pmatrix}=k_1\begin{pmatrix}c\tau^n & 0\\ 0 & c\end{pmatrix}k_2,\ c\in\Omega^{\times}, k_j\in\mathfrak{K}.$$

By the uniqueness of the elementary divisors up to permutations and multiplications by units, this implies $\tau^m=u\tau^nc$ and $1=vc$ with $u,v\in\mathfrak{U}$ or else $\tau^m=uc$ and $1=v^nc$. In the first case, we have $\operatorname{ord}(c)=0$, hence $m=n$; in the second case, $\operatorname{ord}(c)=-n$, hence $m=-n$. This proves

$$(2.4)\qquad Ky^mK=Ky^nK \text{ if and only if } m=\pm n.$$

Thus G is the disjoint union

$$(2.5)\qquad G=\bigcup_{n=0}^{\infty}Ky^nK.$$

Let $\mathfrak{A}$ be the subgroup of non-singular diagonal matrices of $\mathfrak{G}$ and $\mathfrak{B}$ the subgroup of all matrices $\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$, so that $\mathfrak{A}\mathfrak{B}=\mathfrak{B}\mathfrak{A}$ is the subgroup of non-singular triangular matrices. Let A be the image of $\mathfrak{A}$, B the image of $\mathfrak{B}$ under the natural homomorphism (1.6) of $\mathfrak{G}$ onto G. Then $AB=BA$ is a closed subgroup of G, B a closed normal subgroup of AB, $A\cap B=(1)$ and $AB/B\cong A\cong\Omega^{\times}$. The restriction of the homomorphism (1.6) to $\mathfrak{B}$ is clearly a topological isomorphism of $\mathfrak{B}$ onto B and $\mathfrak{B}$ is obviously topologically isomorphic to the additive group Ω^{+} of the field Ω; hence $B\cong\Omega^{+}$. Using elementary divisors, one sees that

$$(2.6)\qquad G=BAK.$$

If $g\in\mathfrak{G}$ has matrix-coefficients x_{ij}, then

$$|\det x_{ij}|^{-2}\,d\mu(x_{11})\,d\mu(x_{12})\,d\mu(x_{21})\,d\mu(x_{22})$$

is easily seen to be a Haar-measure on $\mathfrak{G}$ which is both left- and right-invariant. Hence the Haar-measure on G is both left- and right-invariant, as follows at once from elementary properties of measures on homogeneous spaces. We denote the Haar-measure on G by $\mathfrak{M}$ and write often dg instead of $d\mathfrak{M}g$.

We wish to compute the Haar-measure $\mathfrak{M}(Ky^nK)$ of the compact open subset Ky^nK of G. Clearly, $\bigcup_{k\in K}kgK$ is a compact subset of the coset space G/K; but G/K is discrete, so this is a finite subset of G/K. Hence there exist a finite number r of elements k_j of K such that $KgK=\bigcup_{j=1}^{r}k_jgK$.

or, formally,

$$\mathfrak{F}(\alpha) = \int_G f(\gamma) M(\gamma, \alpha) \, d\gamma. \tag{3.5}$$

Of course, (3.4) will exist only for suitably restricted functions f and ψ. Let us use the fact (elementary divisors) that every element $g \in G$ can be written in the form $g = ba\kappa$ with $\kappa \in K$, and we obtain

$$[\mathfrak{F}(\alpha)\psi](k) = \int f(\gamma)\psi(k\gamma)\,d\gamma = \int f(k^{-1}g)\psi(g)\,dg$$

$$= \int f(k^{-1}ba\kappa)\psi(ba\kappa)\,dg = \int\int f(k^{-1}ba\kappa)\alpha(a)\psi(\kappa)\,d_r(ba)\,d\kappa,$$

where $d\kappa$ refers to the Haar-measure on K, $d_r(ba)$ to the right-invariant Haar-measure on $BA = AB$, normalized so that

$$dg = d_r(ba)\,d\kappa \text{ when } g = ba\kappa. \tag{3.6}$$

Hence, if we put

$$F_\alpha(k, \kappa) = \int_{AB} f(k^{-1}ba\kappa)\alpha(a)\,d_r(ba) \tag{3.7}$$

and note that any function $\psi(g)$ satisfying (3.2) is determined by its restriction to K, we see that the linear transformation $\mathfrak{F}(\alpha)$ (assuming it exists in a suitable sense) is an integral operator with kernel $F_\alpha(k, \kappa)$ given by (3.7). Thus

$$[\mathfrak{F}(\alpha)\psi](k) = \int_K F_\alpha(k, \kappa)\psi(\kappa)\,d\kappa. \tag{3.8}$$

If, for example, ψ is continuous and f continuous of compact support, the above integrals certainly exist. And our integral operator $\mathfrak{F}(\alpha)$ has a trace given by

$$\text{trace}\,\mathfrak{F}(\alpha) = \int_K F_\alpha(k, k)\,dk = \int_K \int_{AB} f(k^{-1}bak)\alpha(a)\,d_r(ba)\,dk. \tag{3.9}$$

In particular, if $f(k^{-1}gk) = f(g)$ for any $g \in G$, $k \in K$, we obtain

$$\text{trace}\,\mathfrak{F}(\alpha) = \int_K dk \int_{AB} f(ba)\alpha(a)\,d_r(ba) = \mathfrak{M}(K)\int_{AB} f(ba)\alpha(a)\,d_r(ba). \tag{3.10}$$

This well known formula goes, of course, back to Gelfand and Naimark who obtained it first for some of the classical groups over the field of complex numbers.

Using (3.2) and $g = bak$, we see that every $\psi(g) \in \mathfrak{V}_\alpha$ is uniquely determined by its restriction to K. Let us now consider only those functions

$\psi \in \mathfrak{V}_\alpha$ for which $\psi(k) \in L^2(K)$. They form a Hilbert space which we denote by $\mathcal{H}_\alpha$. One sees easily that $M(g,\alpha)$ defines a unitary operator of $\mathcal{H}_\alpha$ if and only if

$$\alpha(y^n) = q^{n(it-\frac{1}{2})} \text{ with } t \text{ real.} \tag{3.11}$$

Let us decompose $\mathcal{H}_\alpha$ with respect to the operators $M(k,\alpha)$ with k varying only over K. Since K is compact, we obtain a decomposition of $\mathcal{H}_\alpha$ into a direct sum of finite dimensional pairwise orthogonal K-invariant K-irreducible subspaces. Let us introduce in each of them an orthonormal basis; their union is a complete orthonormal set in $\mathcal{H}_\alpha$. With respect to this basis of $\mathcal{H}_\alpha$, we form the matrix coefficients of the operator $\mathcal{F}(\alpha)$. Using the Schur orthogonality relations, one sees easily that if $f(g) \in S^0$, then all matrix-coefficients of $\mathcal{F}(\alpha)$ are zero except $\langle \mathcal{F}(\alpha)\psi_\alpha, \psi_\alpha \rangle$, where ψ_α is an element of $\mathcal{H}_\alpha$ satisfying $M(k,\alpha)\psi_\alpha = \psi_\alpha$ for all $k \in K$ and $\langle \psi_\alpha, \psi_\alpha \rangle = 1$. It is known and easily verified that the subspace of $M(k,\alpha)$-invariant elements of $\mathcal{H}_\alpha$ is either 1- or 0-dimensional according as $\alpha(k) = 1$ for all $k \in A \cap K$ or not. Hence, if $f(g) \in S^0$, we have trace $\mathcal{F}(\alpha) = \langle \mathcal{F}(\alpha)\psi_\alpha, \psi_\alpha \rangle$, hence

$$\langle \mathcal{F}(\alpha)\psi_\alpha, \psi_\alpha \rangle = \mathfrak{M}(K) \int_{AB} f(ba)\alpha(a)\, d_r(ba). \tag{3.12}$$

Now let us write

$$\phi(g,\alpha) = \langle M(g,\alpha)\psi_\alpha, \psi_\alpha \rangle, \tag{3.13}$$

and we obtain

$$\text{trace } \mathcal{F}(\alpha) = \langle \mathcal{F}(\alpha)\psi_\alpha, \psi_\alpha \rangle = \int_G f(g)\phi(g,\alpha)\, dg. \tag{3.14}$$

4. The mapping $f \to \bar{f}$. We wish to compute the integral $\bar{f}(a) = \int_B f(ba)\, db$ for integrable spherical functions f, where db refers to the Haar-measure on the group B. The restriction of the homomorphism (1.6) $\mathfrak{G} \to G$ to the subgroup $\mathfrak{B}$ of $\mathfrak{G}$ is a topological isomorphism onto B, so that B is isomorphic to the additive group Ω^+ of Ω, $b \leftrightarrow x$; hence $db = d\mu(x)$, where μ is Haar-measure on Ω^+.

Consider now the matrix C defined by

$$C = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} \tau^n & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \tau^n & 0 \\ x\tau^n & 1 \end{pmatrix}.$$

Let $n \geqq 0$; using elementary divisors, one sees that $C \in \mathcal{K}\begin{pmatrix} \tau^m & 0 \\ 0 & 1 \end{pmatrix}\mathcal{K}$, where

$$m = \begin{cases} n & \text{if } \operatorname{ord}(x) \geqq -n \\ n + 2\operatorname{ord}(x) & \text{if } \operatorname{ord}(x) < -n. \end{cases} \tag{4.1}$$

To this we apply the homomorphism (1.6) of $\mathfrak{G}$ onto G and see that

$$by^n \in Ky^mK, \text{ where } b \leftrightarrow x \tag{4.2}$$

and m is given by (4.1). Let r be any non-negative integer and $f_r(g)$ the characteristic function of the double coset Ky^rK, so that $f_r(g)$ is a continuous function on G of compact support. We have

$$f_r(by^n) = \delta_{r,|m|} = \begin{cases} 1 \text{ if } r = |m| \\ 0 \text{ if } r \neq |m|. \end{cases} \tag{4.3}$$

Hence

$$\bar{f}_r(y^n) = \int_B f_r(by^n)\,db = \int_{\operatorname{ord}(x) \geqq -n} \delta_{r,n}\,d\mu(x) + \int_{\operatorname{ord}(x) < -n} \delta_{-r,n+2\operatorname{ord}(x)}\,d\mu(x).$$

Now

$$\int_{\operatorname{ord}(x) \geqq -n} d\mu(x) = q^n\mu(\mathfrak{D})$$

and

$$\int_{\operatorname{ord}(x) < -n} \delta_{-r,n+2\operatorname{ord}(x)}\,d\mu(x) = \begin{cases} 0 & \text{if } r \leqq n \\ \displaystyle\int_{\operatorname{ord}(x) = -(r+n)/2} d\mu(x) & \text{if } r > n \end{cases}$$

since $\operatorname{ord}(x) = -\frac{1}{2}(r+n) < -n$ implies $r > n$. In particular, the last integral is zero if $r+n$ is odd since $\operatorname{ord}(x)$ takes on only rational integers as values. Therefore

$$\int_{\operatorname{ord}(x) < -n} \delta_{-r,n+2\operatorname{ord}(x)}\,d\mu(x) = \begin{cases} 0 & \text{if } r \leqq n \text{ or } r+n \text{ odd} \\ (1-1/q)\,q^{(r+n)/2}\mu(\mathfrak{D}) & \text{if } r > n \text{ and } r+n \text{ even.} \end{cases}$$

Hence

$$\bar{f}_r(y^n) = \begin{cases} q^n\mu(\mathfrak{D}) & \text{if } r = n \geqq 0 \\ 0 & \text{if } 0 \leqq r < n \text{ or if } r+n \text{ is odd} \\ (1-1/q)\,q^{(r+n)/2}\mu(\mathfrak{D}) & \text{if } r > n \geqq 0 \text{ and } r+n \text{ is even.} \end{cases} \tag{4.4}$$

Now let $f(g)$ be any integrable spherical function, then $f(g) = \sum_{r=0}^{\infty} f(y^r) f_r(g)$, and we obtain for $n \geqq 0$ and any $f \in S^1$

$$\begin{aligned} \bar{f}(y^n) &= \sum_{r=0}^{\infty} f(y^r)\,\bar{f}_r(y^n) \\ &= \mu(\mathfrak{D})\{q^n f(y^n) + (1-1/q) \sum_{\substack{r>n \\ r+n \text{ even}}} q^{(r+n)/2} f(y^r)\} \\ &= \mu(\mathfrak{D})\{q^n f(y^n) + (1-1/q) \sum_{j=1}^{\infty} q^{n+j} f(y^{n+2j})\}. \end{aligned}$$

Thus

$$\bar{f}(y^n) = \mu(\mathfrak{D})\,q^n\{f(y^n) + (1-1/q) \sum_{j=1}^{\infty} f(y^{n+2j})\,q^j\}. \tag{4.5}$$

Now consider by^{-n} for $n \geqq 0$. We have, again by elementary divisors, $by^{-n} \in Ky^mK$ where

$$m = \min\{-n, -n + 2\operatorname{ord}(x)\} = \begin{cases} -n & \text{if} \quad \operatorname{ord}(x) \geqq 0 \\ -n + 2\operatorname{ord}(x) & \text{if } \operatorname{ord}(x) < 0. \end{cases}$$

Hence, if $f_r(g)$ is again the characteristic function of the double coset Ky^rK with $r \geqq 0$, we obtain for $n \geqq 0$

$$\int_B f_r(by^{-n})\,db = \int_{\operatorname{ord}(x)\geqq 0} \delta_{r,n}\,d\mu(x) + \int_{\operatorname{ord}(x)<0} \delta_{r,n-2\operatorname{ord}(x)}\,d\mu(x).$$

Now

$$\int_{\operatorname{ord}(x)<0} \delta_{r,n-2\operatorname{ord}(x)}\,d\mu(x) = \begin{cases} \displaystyle\int_{\operatorname{ord}(x)=(n-r)/2} d\mu(x) & \text{if } n-r \text{ is even and } < 0 \\ 0 & \text{otherwise.} \end{cases}$$

Thus for $r \geqq 0$ and $n \geqq 0$

$$\bar{f}_r(y^{-n}) = \begin{cases} \mu(\mathfrak{D}) & \text{if } r = n \\ (1 - 1/q)\,q^{(r-n)/2}\mu(\mathfrak{D}) & \text{if } n - r \text{ is even and } < 0 \\ 0 & \text{otherwise.} \end{cases}$$

We compare this with the above expression (4.4) for $\bar{f}_r(y^n)$ and see that

$$\bar{f}_r(y^{-n}) = q^{-n}\bar{f}_r(y^n). \tag{4.6}$$

We wish to invert the mapping $f \to \bar{f}$. For this purpose, we note that (4.5) implies

$$\bar{f}(y^{n+2}) - q\bar{f}(y^n) = \mu(\mathfrak{D})\,q^{n+1}\{f(y^{n+2}) - f(y^n)\},$$

hence

$$\begin{aligned} f(y^n) &= [f(y^n) - f(y^{n+2})] + [f(y^{n+2}) - f(y^{n+4})] \\ &\qquad + [(y^{n+4}) - f(y^{n+6})] + \cdots \\ &= \mu(\mathfrak{D})^{-1}q^{-(n+1)}[q\bar{f}(y^n) - \bar{f}(y^{n+2})] + q^{-(n+3)}[q\bar{f}(y^{n+2}) \\ &\qquad - \bar{f}(y^{n+4})] + \cdots \\ &= \mu(\mathfrak{D})^{-1}\{\bar{f}(y^n) + (1/q - 1)[\bar{f}(y^{n+2})q^{-1} + \bar{f}(y^{n+4})q^{-3} \\ &\qquad + \bar{f}(y^{n+6})q^{-5} + \cdots]\}. \end{aligned}$$

Thus

$$f(y^n) = \mu(\mathfrak{D})^{-1}q^{-n}\{\bar{f}(y^n) + (1 - q)\sum_{j=1}^{\infty}\bar{f}(y^{n+2j})q^{-2j}\}. \tag{4.7}$$

Let us note that $f(g) \in S^0$ if and only if $f(y^n)$ is zero except for a finite number of n and that (4.5), (4.6) and (4.7) show that this is equivalent to $\bar{f}(y^n)$ vanishing for a finite number of n. Hence, we obtain the following result.

PROPOSITION 4.1. *The mapping $f \to \bar{f}$ maps the space S^0 of all spherical functions of compact support one-one linearly onto the space of all finite sequences $\bar{f}(y^n)$ which satisfy $\bar{f}(y^{-n}) = q^{-n}\bar{f}(y^n)$. The explicit form of the mapping $f \to \bar{f}$ is given by (4.5), it inverse by (4.7).*

5. The mapping $f \to F(s)$. Now we consider

$$F(\alpha) = \mathfrak{M}(K) \int_A \bar{f}(a)\alpha(a)\,d\mu^\times(a),$$

where $\mu^\times$ is the Haar-measure on $\Omega^\times \cong A$ and $\alpha(a)$ a (not necessarily unitary) character of A such that

$$\alpha(ky^n) = \alpha(y^n) \text{ for } k \in A \cap K. \tag{5.1}$$

We write

$$\alpha(y^n) = \alpha_s(y^n) = q^{n(s-1)} \tag{5.2}$$

and $F(s)$ instead of $F(\alpha)$:

$$F(s) = \mathfrak{M}(K) \int_A \bar{f}(a)\alpha_s(a)\,d\mu^\times(a) = \mathfrak{M}(K)\mu^\times(\mathfrak{U}) \sum_{n=-\infty}^{\infty} \bar{f}(y^n)q^{n(s-1)} \tag{5.3}$$

since $f(ky^n) = f(y^n)$ for $k \in A \cap K$. Now we use (4.6) and obtain

$$\begin{aligned} F(s) &= \mathfrak{M}(K)\mu^\times(\mathfrak{U})\{\bar{f}(1) + \sum_{n=1}^{\infty} \bar{f}(y^n)[q^{n(s-1)} + q^{-n}q^{-n(s-1)}]\} \\ &= \mathfrak{M}(K)\mu^\times(\mathfrak{U})\{\bar{f}(1) + \sum_{n=1}^{\infty} \bar{f}(y^n)[q^{n(s-1)} + q^{-ns}]\}. \end{aligned} \tag{5.4}$$

This proves

LEMMA 5.1. *If $f \in S^1$, then $F(s)$ defined by (5.3) satisfies*

$$F(s) = F(1-s) \tag{5.5}$$

for any complex number s for which (5.3) exists.

Now let f vary over S^0; then we know by Proposition 4.1 that $\bar{f}(y^n)$ varies over all finite sequences satisfying $\bar{f}(y^{-n}) = q^{-n}\bar{f}(y^n)$ for $n \geqq 0$. Hence (5.4) shows that $F(s)$ varies over all Fourier polynomials which satisfy $F(s) = F(1-s)$. It is clear that the mapping $f \to F(s)$ is linear. Since $g \to M(g, \alpha)$ is a representation of G, it follows that to the convolution of any two elements of S^0 corresponds the ordinary product of the corresponding functions $F(s)$. This proves

THEOREM 5.1. *The mapping* $f\to F(s)$ *is an isomorphism of the algebra* S^0 *onto the algebra of all polynomials* $F(s)=F(1-s)$ *of the form* $\sum c_n(q^{n(s-\frac{1}{2})}+q^{-n(s-\frac{1}{2})})$. *Hence every maximal ideal of* S^0 *is given by a complex number* c *and is the set* J_c *of all those* $f\in S^0$ *for which* $F(s)$ *vanishes for this* c. *Two maximal ideals* J_c, $J_{c'}$ *are equal if and only if* $c'=c+2\pi in/\log q$ *or* $c'=1-c+2\pi in/\log q$.

In (5.4), let $s=\frac{1}{2}+it$, where t is real. We obtain

$$F(\tfrac{1}{2}+it)=\mathfrak{M}(K)\mu^{\times}(\mathfrak{U})\{f(1)+\sum_{n=1}^{\infty}\tilde{f}(y^n)q^{-n/2}[q^{nit}+q^{-nit}]\}$$

$$=\mathfrak{M}(K)\mu^{\times}(\mathfrak{U})\{f(1)+2\sum_{n=1}^{\infty}\tilde{f}(y^n)q^{-n/2}\cdot\cos(nt\log q)\}.$$

Hence, by Fourier series,

$$\tilde{f}(y^n)=\frac{q^{n/2}\log q}{2\pi\mu^{\times}(\mathfrak{U})\mathfrak{M}(K)}\int_0^{2\pi/\log q}F(\tfrac{1}{2}+it)\cos(nt\log q)\,dt \tag{5.6}$$

$$=\frac{q^{n/2}\log q}{\pi\mu^{\times}(\mathfrak{U})\mathfrak{M}(K)}\int_0^{\pi/\log q}F(\tfrac{1}{2}+it)\cos(nt\log q)\,dt \text{ for } n\geqq 0.$$

In (4.5), let us replace $f(g)$ by $f^*(g)=\bar{f}(g^{-1})$ and* note that $f(g)=f(g^{-1})$ for $f(g)\in S$. We obtain

$$\tilde{f}^*(y^n)=\mu(\mathfrak{D})q^n\{\bar{\tilde{f}}(y^n)+(1-1/q)\sum_{j=1}^{\infty}\bar{\tilde{f}}(y^{n+2j})q^j\}.$$

Hence, if we write $h(y^n)=\tilde{f}(y^n)$, we have

$$\tilde{f}^*(y^n)=\bar{h}(y^n).$$

Now we put that in (5.4) and write $F^*(s)=\mathfrak{M}(K)\int_A\tilde{f}^*(a)\alpha_s(a)\,d\mu^{\times}(a)$. We obtain

$$F^*(s)=\mathfrak{M}(K)\mu^{\times}(\mathfrak{U})\{\bar{h}(1)+\sum_{n=1}^{\infty}\bar{h}(y^n)[q^{n(s-1)}+q^{-ns}].$$

Therefore

$$\bar{F}^*(\bar{s})=\mathfrak{M}(K)\mu^{\times}(\mathfrak{U})\{\tilde{f}(1)+\sum_{n=1}^{\infty}\tilde{f}(y^n)[q^{n(s-1)}+q^{-ns}].$$

Hence

$$F^*(s)=\bar{F}(\bar{s})\,; \tag{5.7}$$

in particular,

$$F^*(\tfrac{1}{2}+it)=\bar{F}(\tfrac{1}{2}-it)=\bar{F}(\tfrac{1}{2}+it).$$

---

* $\bar{f}$ denotes the complex conjugate of f, whereas $\tilde{f}$ is defined at the beginning of § 4.

If we combine this with Proposition 4.1, we see that $F^*(s) = \bar{F}(s)$ for all $f \in S^0$ if and only if $Rs = \frac{1}{2}$ or $s + 2\pi i n/\log q$ is real.

6. The dual measure. We shall now compute the value of $f \in S^0$ at the unit element 1 of G in terms of $F(s)$. By (4.7), we have

$$f(1) = \mu(\mathfrak{D})^{-1}\{\bar{f}(1) + (1-q)\sum_{j=1}^{\infty}\bar{f}(y^{2j})q^{-2j}\}.$$

Hence, using (5.6), we get

$$f(1) = \frac{\log q}{2\pi\mu(\mathfrak{D})\mu^{\times}(\mathfrak{U})\mathfrak{M}(K)} \int_0^{2\pi/\log q} F(\tfrac{1}{2}+it)\,[1 + (1-q)\sum_{n=1}^{\infty} q^{-n}\cos(2nt\log q)]\,dt.$$

Now we use (2.11), i.e., $\mu(\mathfrak{D})\mu^{\times}(\mathfrak{U}) = 1$, and get

$$f(1) = \frac{\log q}{\pi\mathfrak{M}(K)}\int_0^{\pi/\log q} F(\tfrac{1}{2}+it)\,[1 + (1-q)\sum_{n=1}^{\infty} q^{-n}\cos(2nt\log q)]\,dt.$$

Noting that

$$\sum_{n=1}^{\infty} q^{-n}\cos(2nt\log q) = \tfrac{1}{2}\left\{\frac{q^{2i}}{q-q^{2it}} + \frac{q^{-2it}}{q-q^{-2it}}\right\},$$

we obtain

$$f(1) = \int_0^{\pi/\log q} F(\tfrac{1}{2}+it)\,\mathfrak{M}^*(\tfrac{1}{2}+it)\,dt, \tag{6.1}$$

where

$$\begin{aligned}\mathfrak{M}^*(s) &= \frac{\log q}{\pi\mathfrak{M}(K)}\left[1 + \frac{1-q}{2}\left(\frac{q^{2s-1}}{q-q^{2s-1}} + \frac{q^{1-2s}}{q-q^{1-2s}}\right)\right] \\ &= -\frac{\log q}{\pi\mathfrak{M}(K)}\cdot\frac{q(q+1)}{2}\cdot\frac{(q^{s-\frac{1}{2}}-q^{\frac{1}{2}-s})^2}{(q^{2s-1}-q)(q^{1-2s}-q)}.\end{aligned}$$

In particular, for $s = \frac{1}{2} + it$,

$$\mathfrak{M}^*(\tfrac{1}{2}+it) = -\frac{\log q}{\pi\mathfrak{M}(K)}\cdot\frac{q(q+1)}{2}\;\frac{(q^{i}-q^{-it})^2}{(q^{2it}-q)(q^{-2it}-q)},$$

thus

$$\mathfrak{M}^*(\tfrac{1}{2}+it) = \frac{2q(q+1)\log q}{\pi\mathfrak{M}(K)}\cdot\frac{\sin^2(t\log q)}{1-2q\cos(2t\log q)+q^2}. \tag{6.3}$$

Hence

$$\mathfrak{M}^*(\tfrac{1}{2}+it) \geqq 0 \text{ for real } t. \tag{6.4}$$

We note that

$$\mathfrak{M}^*(\tfrac{1}{2}+\frac{i\pi n}{\log q}) = 0 \quad \text{for } n = 0, \pm 1, \pm 2, \cdots. \tag{6.5}$$

LEMMA 6.1. *The function* $\mathfrak{M}^*(s)$ *is a meromorphic function of* s *(in fact, a rational function of* q^s*), regular in* s *except when* $q^s = \pm q$ *or* $q^s = \pm 1$ (i. e., $s = \pi i n/\log q$ *or* $s = 1 + \pi i n/\log q$) *where it has a pole of order* 1 *with residue*

$$\frac{1-q}{4\mathfrak{M}(K)\pi}. \tag{6.6}$$

It satisfies the functional equation $\mathfrak{M}^*(1-s) = \mathfrak{M}^*(s)$. *Moreover,* $\mathfrak{M}^*(s) \geqq 0$ *for* $Rs = \frac{1}{2}$.

7. The Plancherel formula for S^2. Let $f(g) \in S^0$, and put, as usual $f^*(g) = \bar{f}(g^{-1})$; then $(f * f^*)(g) \in S^0$, where $*$ denotes convolution on G. If to f corresponds $F(\frac{1}{2}+it)$ in the sense of (5.3), then to f^* corresponds $\bar{F}(\frac{1}{2}+it)$, because $g \rightarrow M(g, \frac{1}{2}+it)$ is a unitary representation of G if t is real (see § 3 or equation (5.7) above). Hence to $f * f^*$ corresponds the function* $|F(\frac{1}{2}+it)|_\infty^2$. To this we apply (6.1) and obtain

$$(f * f^*)(1) = \int_0^{\pi/\log q} |F(\tfrac{1}{2}+it)|_\infty^2 \mathfrak{M}^*(\tfrac{1}{2}+it)\,dt.$$

Next we observe that $(f * f^*)(1) = \int_G |f(g)|_\infty^2\,dg$ and that $F(\frac{1}{2}+it)$ is even in t and periodic with period $2\pi/\log q$. Hence

$$\int_G |f(g)|_\infty^2\,dg = \int_0^{\pi/\log q} |F(\tfrac{1}{2}+it)|_\infty^2 \mathfrak{M}^*(\tfrac{1}{2}+it)\,dt. \tag{7.1}$$

Clearly S^0 is dense in S^2. On the other hand, by Theorem 5.1, $F(\frac{1}{2}+it)$ varies over all even Fourier polynomials in t with period $2\pi/\log q$ as f varies over S^0. Hence (7.1) shows that the mapping $f(g) \rightarrow F(\frac{1}{2}+it)$ can be extended uniquely to a unitary mapping of S^2 onto the Hilbert space of all equivalence classes of complex-valued functions which are square integrable over the interval $0 \leqq t \leqq \pi/\log q$ relative to the measure $\mathfrak{M}^*(\frac{1}{2}+it)\,dt$.

8. The elementary spherical function $\varphi(g, s)$. Combining (4.7) with (5.6), we obtain

$$\begin{aligned} f(y^n) &= \frac{\log q}{\pi q^n \mathfrak{M}(K)\mu(\mathfrak{D})\mu^\times(\mathfrak{U})} \int_0^{\pi/\log q} F(\tfrac{1}{2}+it)\{q^{n/2}\cos(nt\log q) \\ &\qquad + (1-q)\sum_{j=1}^\infty q^{n/2-j}\cos[(n+2j)t\log q]\}\,dt \\ &= \frac{q^{-n/2}\log q}{\pi\mathfrak{M}(K)} \int_0^{\pi/\log q} F(\tfrac{1}{2}+it)\{q^{n/2}\cos(nt\log q) \\ &\qquad + (1-q)\sum_{j=1}^\infty q^{-j}[(n+2j)t\log q]\}\,dt, \end{aligned}$$

---

* $|\ |_\infty$ denotes the ordinary absolute value of a complex number.

using (2.11), i.e., $\mu(\mathfrak{D})\mu^{\times}(\mathfrak{U})=1$. Now

$$\cos(nt\log q)+(1-q)\sum_{j=1}^{\infty}q^{-j}\cos[(n+2j)t\log q]$$

$$=\tfrac{1}{2}\left\{q^{int}+q^{-int}+(1-q)\left[q^{int}\cdot\frac{q^{2it}}{q-q^{2it}}+q^{-int}\cdot\frac{q^{-2it}}{q-q^{-2it}}\right]\right\}$$

$$=\tfrac{1}{2}\left\{q^{int}\cdot\frac{q-q^{2it+1}}{q-q^{2it}}+q^{-int}\cdot\frac{q-q^{1-2it}}{q-q^{-2it}}\right\}.$$

We divide this expression by $\mathfrak{M}^*(\tfrac{1}{2}+it)$ and obtain

$$-\frac{\pi\mathfrak{M}(K)}{q(q+1)\log q}\left\{q^{int}\cdot\frac{q^{1-it}-q^{2+it}}{q^{i}-q^{-it}}+q^{-int}\cdot\frac{q^{1+it}-q^{2-it}}{q^{-it}-q^{it}}\right\}.$$

Hence

$$f(y^n)=\int_0^{\pi/\log q}F(\tfrac{1}{2}+it)\phi(y^n,\tfrac{1}{2}+it)\mathfrak{M}^*(\tfrac{1}{2}+it)\,dt, \tag{8.1}$$

where, for $n\geqq 0$,

$$\phi(y^n,s)=\frac{q^{n(s-\frac{1}{2})}[q^{\frac{3}{2}+s}-q^{\frac{3}{2}-s}]-q^{-n(s-\frac{1}{2})}[q^{\frac{5}{2}-s}-q^{\frac{1}{2}+s}]}{(q+1)q^{n/2+1}(q^{s-\frac{1}{2}}-q^{\frac{1}{2}-s})}. \tag{8.2}$$

One sees at once that $\phi(y^n,s)$ is, for fixed n, an entire function of s (including at $s=\tfrac{1}{2}+\pi in/\log q$). Hence, we obtain, for each fixed complex number s, a spherical function $\phi(g,s)$ on G by putting $\phi(k_1y^nk_2,s)=\phi(y^n,s)$ for any $k_j\in K$ and using (2.3), (2.4) and (2.5). By putting $n=0$ in (8.2), one sees that

$$\phi(1,s)=1 \text{ for all } s. \tag{8.3}$$

By putting $s=0$ or 1 in (8.2), one sees that

$$\phi(g,0)=\phi(g,1)=1 \text{ for all } g\in G. \tag{8.4}$$

Moreover, (8.2) implies immediately the functional equation

$$\phi(g,s)=\phi(g,1-s) \text{ for all } g\in G. \tag{8.5}$$

Also,

$$\bar{\phi}(g,\tfrac{1}{2}+it)=\phi(g,\tfrac{1}{2}+it) \text{ for real } t. \tag{8.6}$$

Hence, if we combine (7.1) and (8.1), we may conclude that

$$F(\tfrac{1}{2}+it)=\int_G f(g)\phi(g,\tfrac{1}{2}+it)\,dg \tag{8.7}$$

for all $f(g)\in S^0$, or for all $f(g)\in S^2$ if one introduces the usual l.i.m. $\int$. So we see that if $f(g)\in S^0$, then

$$F(s) = \int_G f(g)\phi(g,s)\,dg. \tag{8.8}$$

If we combine this with (3.14), we see that $\phi(g,s) = \phi(g,\alpha)$ provided α satisfies (5.1) and (5.2). Now from (8.2), we obtain at once that

$$|\phi(g,s)| \leqq \phi(g,\sigma), \text{ where } \sigma = Rs. \tag{8.9}$$

Hence, combining (8.4) with (8.9), we obtain

$$|\phi(g,it)| \leqq 1 \quad \text{and} \quad |\phi(g,1+it)| \leqq 1. \tag{8.10}$$

It follows from this that, for all $g \in G$,

$$|\phi(g,s)| \leqq 1 \quad \text{for } 0 \leqq Rs \leqq 1. \tag{8.11}$$

We now prove that $\phi(g,s)$ is an unbounded function of g for any fixed s for which $Rs > 1$ or $Rs < 0$. Indeed,

$$\frac{q^{n(s-\frac{1}{2})}[q^{\frac{3}{2}+s} - q^{\frac{3}{2}-s}]}{(q+1)q^{n/2+1}(q^{s-\frac{1}{2}} - q^{\frac{1}{2}-s})} + \frac{q^{n(s-1)}[q^s - q^{-s}]q^{\frac{1}{2}}}{(q+1)(q^{s-\frac{1}{2}} - q^{\frac{1}{2}-s})} \to +\infty$$

as $n \to +\infty$ if $Rs = \sigma > 1$, whereas

$$\frac{q^{-n(s-\frac{1}{2})}[q^{\frac{5}{2}-s} - q^{\frac{1}{2}+s}]}{(q+1)q^{n/2+1}(q^{s-\frac{1}{2}} - q^{\frac{1}{2}-s})} + \frac{q^{-ns}[q^{\frac{5}{2}-s} - q^{\frac{1}{2}+s}]}{q(q+1)(q^{s-\frac{1}{2}} - q^{\frac{1}{2}-s})} \to 0$$

as $n \to +\infty$ if $Rs = \sigma > 0$. Therefore $\phi(y^n, s)$ is unbounded as $n \to +\infty$ for any fixed s with $Rs > 1$, hence, because of (8.5), also for $Rs < 0$.

On the other hand, if $0 < Rs < 1$, then $q^{\pm n(\sigma-\frac{1}{2})\pm int}\, q^{-n/2} \to 0$ as $n \to +\infty$. Therefore

$$\lim_{n\to+\infty} \phi(y^n, s) = 0 \text{ if } 0 < Rs < 1 \tag{8.12}$$

uniformly in s for $\epsilon \leqq Rs \leqq 1 - \epsilon$, $\epsilon > 0$. This proves

LEMMA 8.1. *$\phi(g,s)$ is an unbounded function of g for any fixed complex number s for which $Rs > 1$ or $Rs < 0$.*

On the other hand, $|\phi(g,s)| \leqq 1$ for all $g \in G$ if $0 \leqq Rs \leqq 1$, and (8.12) *holds.*

From this we deduce

THEOREM 8.1. *Let $f(g) \in S^1$, then $F(s) = \int f(g)\phi(g,s)\,dg$ is a regular analytic function in the strip $0 < Rs < 1$, continuous in $0 \leqq Rs \leqq 1$, satisfying*

$$F(s) = F(1-s) = F\left(s + \frac{2\pi i n}{\log q}\right). \tag{8.13}$$

Any homomorphism of the commutative normed algebra S^1 *to the complex numbers is of the form* $f(g) \rightarrow \int f(g)\phi(g,c)\,dg = F(c)$, *where* c *is a complex number in the strip* $0 \leqq Rc \leqq 1$. *This homomorphism maps* $f^*(g) = \bar{f}(g^{-1})$ *to* $\bar{F}(c)$ *if and only if* $Rc = \frac{1}{2}$ *or* $c + 2\pi in/\log q$ *is real. Two homomorphisms* $f \rightarrow F(c)$ *and* $f \rightarrow F(c')$ *are identical if and only if* $c' = c + 2\pi in/\log q$ *or* $c' = 1 - c + 2\pi in/\log q$.

Proof. The regularity and continuity of $F(s)$ follow immediately from the above properties of $\phi(g,s)$, and so does (8.13). Now given any homomorphism of S^1 to the complex numbers, its restriction to S^0 is, of course, a homomorphism of S^0 to the complex numbers, hence, by Theorem 5.1 above, is of the form $f \rightarrow F(c)$ for some complex number c. In order that this homomorphism can be extended to a homomorphism of S^1, it is necessary and sufficient that $\phi(g,c)$ be a bounded function of g for this number c. Hence, by Lemma 8.1, we must have $0 \leqq Rc \leqq 1$. The assertion about the identity of two such homomorphisms follows from the corresponding assertion about S^0 (see again Theorem 5.1) above). The assertion about $f^*(g)$ follows immediately from the last assertion in § 5 above (see equation (5.7) above) and Theorem 5.1.

THE JOHNS HOPKINS UNIVERSITY.

CHARACTERISTIC CLASSES AND HOMOGENEOUS SPACES, I.*

By A. Borel and F. Hirzebruch.

Introduction. It is known that the characteristic classes of a real or complex vector bundle may be interpreted as elementary symmetric functions in certain variables, which are 1, 2 or 4 dimensional cohomology classes. If we consider the tangent bundle of the coset space G/U of a compact connected Lie group modulo a closed subgroup, it turns out that these variables may be identified with certain roots of G (or their squares). Our first purpose is to establish this connection between roots and characteristic classes, which is the basis of this paper, and to compute the characteristic classes of certain well-known homogeneous spaces. These results are then applied in particular to G/T (T maximal torus of G), and to other algebraic homogeneous spaces, where they lead to relations between characteristic classes, Betti numbers, the Riemann-Roch theorem and representation theory; they are also used to discuss multiplicative properties of the Todd genus and other genera in fibre bundles with G/U as fibre. As an application, we get a divisibility property of the Chern class of a complex vector bundle over an even dimensional sphere which yields some information about certain homotopy groups of Lie groups.

We now give a summary of the different chapters. For the notions and notations used without further comments, the reader is referred to [2, 19].

Chapter I. The first three Sections give a survey of standard properties of roots and linear representations; § 4 gives two characterizations of systems of positive roots which will be used in Chapter IV. In § 5 we introduce the roots of a Lie group with respect to a commutative subgroup of type $(2, 2, \cdots, 2)$, which will occur in the description of Stiefel-Whitney classes.

Chapter II recalls those concepts of fibre bundle theory which are most often used in this paper, such as restriction and extension of the structural group (with respect to homomorphisms), integration over the fibre, to be denoted by $\natural$, and the bundle of vectors tangent to the fibres of a bundle whose typical fibre admits a differentiable structure invariant under the structural group, to be called hereafter the "bundle along the fibres".

---

* Received January 29, 1958.

Chapter III starts with a review of the definition by means of symmetric functions of the characteristic classes of a bundle having a classical group as structural group (§ 9). In § 10, we consider the λ-extension η^λ of a principal G-bundle η by means of a unitary representation $\lambda\colon G \to U(n)$; the bundle η^λ is a principal $U(n)$-bundle, whose Chern classes are shown to be the elementary symmetric functions in the weights of λ, suitably interpreted as 2-dimensional classes; analogous statements are proved for the real orthogonal representations and Pontrjagin classes (10.3). Now, the real tangent bundle to G/U is the ι-extension of the principal U-bundle $(G, G/U, U)$, with respect to the linear isotropy representation ι of U in the tangent space at a point of G/U fixed under U (Proposition 7.5). Applying 10.3 to this situation yields the relation between roots and characteristic classes mentioned at the beginning of this introduction, which, in fact, holds more generally for the bundle along the fibres of $(E/U, B, G/U)$, where (E, B, G) is a principal G-bundle.

Chapter IV. The homogeneous space G/U admits an invariant almost complex structure J if and only if the isotropy representation ι can be factorized through the standard inclusion of $\boldsymbol{U}(n)$ in $\boldsymbol{SO}(2n)$, $(2n = \dim G/U)$; we obtain in this case a unitary representation $\iota_c\colon U \to \boldsymbol{U}(n)$, whose weights are certain roots of G, to be called the roots of J; they allow us to compute the Chern classes of J using 10.3 and to discuss the integrability of J using the results of § 4; among the applications in § 13 we give new proofs of some results of H. C. Wang.

The invariant complex structures of G/U (where U is the centralizer of a torus in G), can be obtained directly by using the complexification of G; the space G/U is also homogeneous kählerian [5] and even rational algebraic, and there is a close connection between its projective embeddings and the linear representations of G. For later use, we include in § 14 a short discussion of some of these results; moreover, we prove (14.10) that the real cohomology classes of these algebraic homogeneous spaces are all of type (p, p) and for $p = 1$ describe those which are positive in the sense of Kodaira.

Chapter V is devoted to some special cases; in particular, to projective spaces.

Chapter VI.† In § 20 a formula for the homomorphism $\natural$ in the bundle $\xi = (B_T, B_G, G/T, \rho(T, G))$ is established (20.3); it shows, in particular (22.2), that $\natural$, applied to the total Todd class of the bundle along the fibres of ξ endowed with the complex vector bundle structure defined by means of an invariant almost complex structure J on G/T, gives a zero-dimensional term, which is 1 or 0, according to whether J is integrable or not; it follows that the Todd genus $T(G/T)$[1] of G/T with respect to J is 1 or zero respectively and that (22.5) in certain bundles $(E, B, G/T)$, with almost complex E and B the Todd genus, "behaves multiplicatively," i.e., that we have $T(E) = T(B) \cdot T(F)$. These results are generalized to the T_y-genus and to homogeneous almost complex spaces G/U (rank $U =$ rank G).

---

† §§ 20 to 30 will be published in a later issue of this Journal.

In § 23 we consider the A-genus of homogeneous spaces G/U with rank $U =$ rank G and, in particular, prove it to be equal to 0 when the second Betti number of G/U vanishes; moreover, in a differentiable bundle $(E/U, B, G/U)$ with $A(G/U) = 0$, we also have $A(E) = 0$.

In § 24, G/U (rank $U =$ rank G) is assumed to be algebraic. The value of the T_y-genus found in § 22 and (14.10) yield a formula for the Betti numbers of G/U in terms of the action of the Weyl groups of G and U on the roots of G. The dimension of the vector space of holomorphic cross-sections of a complex line bundle F on G/U is computed by means of the Riemann-Roch theorem and is shown to be either zero or equal to the degree of the irreducible representation of G having the first Chern class of F as highest weight (24.7); (this fact has led to the results of [7a] and has been further generalized by R. Bott [7b]). The degree (in the sense of algebraic geometry) of the projective embedding of G/U given by this linear representation, or equivalently, by the complete linear system of divisors belonging to F, is also explicitly calculated.

Chapter VII. In § 25, the A-genus is proved to be an integer. More generally, we introduce, for a complex vector bundle η over a differentiable manifold X and for an arbitrary element $d \in H^2(X, \mathbf{Z})$, a rational number $\hat{A}(X, d, \eta)$, in analogy with the Riemann-Roch formula, and prove that it is an integer after multiplication by a suitable power of 2. It follows that the q-th Chern class of a complex vector bundle over the $2q$-dimensional sphere S_{2q} is divisible by the greatest odd factor of $(q-1)!$; applications of this last fact to the homotopy of Lie groups are given in § 26.

As is well known, the index of a differentiable manifold X equals the L-genus of X, which is a linear combination of Pontrjagin numbers [19]. It was recently proved [12] that the index "behaves multiplicatively" in differentiable bundles. This fact has certain consequences for the Pontrjagin classes of the bundle along the fibres of a differentiable bundle, from which we conclude that the sequence of L-polynomials is essentially uniquely characterized by the property of giving rise to a genus which behaves multiplicatively in differentiable fibre bundles.

---

[1] We allow ourselves to denote by T the Todd genus as well as a maximal torus, since this is unlikely to bring any confusion.

In Appendix I, we compare the different definitions of Chern classes known to us, with particular emphasis on the signs.

In Appendix II, it is first proved that the torsion coefficients of $H^*(B_{\mathbf{O}(n)}, \mathbf{Z})$ and $H^*(B_{\mathbf{SO}(n)}, \mathbf{Z})$ are all of order 2. This allows us to characterize the universal *integral* Pontrjagin class p_i by its canonical images in $H^{4i}(B_{\mathbf{O}(n)}, \mathbf{R})$ and $H^{4i}(B_{\mathbf{O}(n)}, \mathbf{Z}_2)$, the latter being equal to the square of the universal $2i$-th Stiefel-Whitney class. It is also shown that, up to 2-torsion, the integral i-th Pontrjagin class of a principal $\mathbf{O}(n)$-bundle ξ can be defined by means of the transgression in a certain bundle η_i associated with ξ; in particular, η_i has the typical fibre $\mathbf{O}(n)/\mathbf{O}(2i-1)$ when n is odd.

TABLE OF CONTENTS

CHAPTER I. COMPACT LIE GROUPS

§ 1. Generalities
§ 2. Standard properties of roots
§ 3. Linear representations
§ 4. Two characterizations of systems of positive roots
§ 5. The 2-roots of a compact Lie group

CHAPTER II. TOPOLOGICAL PRELIMINARIES

§ 6. Fibre bundles
§ 7. Vector bundles
§ 8. Integration over the fibre

CHAPTER III. ROOTS AND CHARACTERISTIC CLASSES

§ 9. Characteristic classes
§ 10. Representations and Characteristic classes
§ 11. Representations and Stiefel-Whitney classes

CHAPTER IV. ROOTS AND INVARIANT ALMOST COMPLEX STRUCTURES

§ 12. The integrability of invariant almost complex structures
§ 13. Applications
§ 14. Complex Lie groups. Embeddings, representations, invariant differential forms.

CHAPTER V. SPECIAL CASES

§ 15. Projective spaces
§ 16. Hermitian symmetric spaces
§ 17. The Stiefel-Whitney class of $\boldsymbol{G_2/SO}(4)$
§ 18. Some manifolds with Poincaré polynomial $1 + t^4 + t^8$
§ 19. The Cayley plane

CHAPTER VI. APPLICATIONS TO TODD GENERA

§ 20. Integration over the fibre in $(B_T, B_G, G/T, \rho(T, G))$
§ 21. Multiplicative sequences
§ 22. The Todd genus of certain almost complex homogeneous spaces
§ 23. The A-genus of certain homogeneous spaces
§ 24. Applications to simply connected algebraic homogeneous spaces

CHAPTER VII. GENERA DEFINED BY PONTRJAGIN CLASSES

§ 25. The integrality of the A-genus
§ 26. Applications to homotopy groups of Lie groups
§ 27. Multiplicative properties of the index and consequences
§ 28. A uniqueness theorem on the index

Appendix I

§ 29. The different definitions of the Chern classes

Appendix II

§ 30. The Pontrjagin classes

Chapter I. Compact Lie Groups.

1. Generalities.

1.1. *Coset spaces.* Let G be a Lie group, U a closed subgroup of G, G/U the space of left cosets of $G \bmod U$, π the natural projection of G onto G/U, and $\mathfrak{g}$, $\mathfrak{u}$ the Lie algebras of G, U identified as usual with the tangent spaces at the neutral element. Left translation by $g \in G$ induces a homeomorphism of G/U which will be denoted by the same letter; if $u \in U$, it leaves $o = \pi(e)$ invariant and induces an automorphism $\tilde{u}$ of the tangent space $(G/U)_0$ of G/U at o. The homomorphism $\iota_u : u \rightarrow \tilde{u}$ is called the ***isotropy representation*** and its image the ***linear isotropy group*** $\tilde{U}$. For connected G, its kernel is the subgroup of those elements of G which act trivially on G/U or, also, the largest subgroup of U invariant in G.

$\mathrm{Ad}\, g$ or $\mathrm{Ad}_{\mathfrak{g}}\, g$ will denote the automorphism of $\mathfrak{g}$ induced by the inner automorphism $x \to gxg^{-1}$ of G. If π_e is the differential of π at e, we have clearly

$$\pi_e \circ \mathrm{Ad}_{\mathfrak{g}}\, u = \tilde{u} \circ \pi_e \qquad (u \in U);$$

in particular, since the kernel of π_e is $\mathfrak{u}$, π_e allows us to identify $(G/U)_0$ with any subspace $\mathfrak{m}$ of $\mathfrak{g}$ supplementary to $\mathfrak{u}$, invariant under $\mathrm{Ad}_{\mathfrak{g}}\, u$, in such a way that $\tilde{u}$ is carried over to the restriction of $\mathrm{Ad}_{\mathfrak{g}}\, u$ to $\mathfrak{m}$. If σ is an automorphism of G and σ_e its differential at e, then

$$\text{(1)} \qquad \mathrm{Ad}\, \sigma(g) = \sigma_e \circ \mathrm{Ad}\, g \circ \sigma_e^{-1}.$$

1.2. From now on, G is a compact Lie group. We recall that its maximal toral subgroups are conjugate to each other by inner automorphisms and are maximal abelian subgroups of G if G is connected; their common dimension is the *rank* of G, to be denoted here by l or $l(G)$. The letter T will be reserved for a maximal torus of G, and S for an arbitrary toral subgroup; V_S will be the universal covering of S and Γ_S the "unit lattice", i.e., the inverse image of the identity element of S. The latter is a free commutative group of rank k ($k = \dim S$), which spans V_S. A real valued linear form on V_S is said to be *integral* if it takes integral values on Γ_S.

1.3. *Roots, diagram.* The representation $s \to \mathrm{Ad}_{\mathfrak{g}}\, s$ of S in $\mathfrak{g}$ is fully reducible and there is a direct sum decomposition

$$\text{(2)} \qquad \mathfrak{g} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_k + \mathfrak{b} + \mathfrak{s} \qquad (\dim \mathfrak{a}_i = 2)$$

of $\mathfrak{g}$ into subspaces invariant under $\mathrm{Ad}_{\mathfrak{g}}\, S$, where $\mathfrak{b} + \mathfrak{s}$ is the largest subspace on which S operates trivially. We may then write, for $s \in S$,

$$\text{(3)} \qquad \mathrm{Ad}_{\mathfrak{g}}\, s \mid \mathfrak{a}_i = \begin{pmatrix} \cos 2\pi a_i(s) & -\sin 2\pi a_i(s) \\ \sin 2\pi a_i(s) & \cos 2\pi a_i(s) \end{pmatrix}$$

where $a_i(p(x))$, p the projection of V_S onto S, is a non-zero integral linear form.[2] The linear forms $\pm a_i$ are *the roots of G with respect to S*. We shall be concerned mainly with the case where $S = T$ is a maximal torus. Then $\mathfrak{b} = 0$, and the $2m$ linear forms $\pm a_i$, $(i = 1, \cdots, m;\ \dim. G = l + 2m)$, are simply *the roots* of G.[3] Clearly, if $S \subset T$, the roots relative to S are the restriction to V_S of the roots of G which do not vanish identically on S.

---

[2] In the sequel, there will be no notational distinction between $a(p(x))$ and $a(t)$.

[3] We call them roots in spite of the facts that the roots in the sense of the

An element $t \in T$ is *singular* if its centralizer has dimension $> l(G)$, *regular* otherwise; in V_T the singular elements are represented by the points of the hyperplanes $a_i \equiv 0 \bmod 1$, $(1 \leqq i \leqq m)$, which form the *diagram of G*.

In case S is a toral subgroup of U, the decomposition (2) may be chosen in such a way that $\mathfrak{u}$ is spanned by a subspace $\mathfrak{h}_1$ of $\mathfrak{h}$, $\mathfrak{s}$ and some of the $\mathfrak{a}_i$, say $\mathfrak{a}_1, \cdots, \mathfrak{a}_q$; the $\pm a_i$ $(q < i \leqq m)$ will be called *the roots* of G *relative* to S *complementary to those of* U, or simply the *complementary roots* if there is no danger of confusion.

1.4. *The Weyl Group.* We choose once and for all a positive definite metric on $\mathfrak{g}$ invariant under $\operatorname{Ad} G$, and consider on V_T the metric which is induced by it in the obvious way; it allows us to define in the standard way a canonical isomorphism between V_T and its dual space $V_T{}^*$ and a metric on $V_T{}^*$; the scalar product on V_T or $V_T{}^*$ will be denoted $(\ ,\ )$. An element $a \in V_T{}^*$ is called *singular* if there exists a root a_i such that $(a, a_i) = 0$; its image in V_T under the canonical isomorphism is then singular in the above sense. Finally, we remark that the symmetry S_a of V_T with respect to the hyperplane $a = 0$ induces a symmetry of $V_T{}^*$, to be denoted also by S_a, defined by

$$S_a(b) = b - 2(a, b)(a, a)^{-1} \cdot a.$$

The Weyl group $W(G)$ of G is the group of automorphisms of T induced by inner automorphisms of G leaving T invariant; it is a finite group and a quotient of N_T/T, where N_T is the normalizer of T in G; it may also be viewed as a group if isometries of V_T leaving Γ_T and the diagram invariant. For connected G, it is isomorphic to N_T/T and is generated by the symmetries to the hyperplanes $a_i = 0$ $(i = 1, \cdots, m)$.

2. Standard properties of roots. G is a compact *connected* Lie group of dimension n and rank l, T a maximal torus, V its universal covering and $\pm a_i$ $(1 \leqq i \leqq m, n = l + 2m)$ are the roots of G. The proofs of the statements in §§ 2, 3 may be found e. g. in [8, 13, 23, 27, 28].

2.1. An element $v \in V$ is in the inverse image of the center of G if and only if $a_i(v) \equiv 0 \bmod 1$ $(i = 1, \cdots, m)$; in particular, G is semi-simple if and only if it has l linearly independent roots.

2.2. a_i and a_j are linearly independent if $i \neq j$.

---

infinitesimal theory (i. e., the roots of the Killing equation), are the forms $\pm 2\pi i a_j$ and the zero form; the forms a_j were called "paramètres angulaires" by E. Cartan [8]. Also, unless otherwise specified, the zero form will not be considered as a root.

2.3. The number $2(a, b) \cdot (a, a)^{-1}$ is an integer for any two roots a, b and the linear forms $b - k \cdot a$ are also roots for k integral varying between 0 and $2(a, b)(a, a)^{-1}$.

2.4. *Simple roots.* Let (x^i), $(1 \leqq i \leqq l)$, be a base of V^*. We define a total ordering $\mathcal{S}$ on V^* by saying that $a = a_1 x^1 + \cdots + a_l x^l$ is > 0 if its first non vanishing coefficient is > 0 and that $a > b$ if $a - b > 0$. A root is *simple,* relative to $\mathcal{S}$, if it is positive and cannot be represented as the sum of two positive non-zero roots. The simple roots are linearly independent, the scalar product of any two of them is $\leqq 0$, and every root is a linear combination, with integral coefficients of the same sign, of simple roots. It follows, in particular, that, when G is semi-simple, there are l simple roots; also, a simple root is not a linear combination with positive coefficients of other positive roots.

2.5. A set of elements of V or V^* is said to be decomposable if it is the union of two non-empty mutually orthogonal subsets. A semi-simple group G is simple if and only if its root system or the system of its simple roots is indecomposable. Assume G to be simple, let a_i $(1 \leqq i \leqq l)$ be the simple roots and let $b = b_1 a_1 + \cdots + b_l a_l$ be the highest root with respect to an ordering $\mathcal{S}$. Then we have

$$(b, a_i) \geqq 0, \qquad b_i > 0, \qquad\qquad (i = 1, \cdots, l),$$

and b_i majorizes the coefficient of a_i for all roots.

2.6. *The sign of an element of* $W(G)$. Let a_i $(1 \leqq i \leqq m)$, be the positive roots with respect to $\mathcal{S}$. Since $W(G)$ leaves the diagram invariant, any $w \in W(G)$ induces a permutation of the system $(\pm a_i)$ $(1 \leqq i \leqq m)$, and transforms (a_i) into a system of roots $(\epsilon_i a_i)$ with $\epsilon_i = \pm 1$. We shall denote by $s(w)$ the number of ϵ_i's equal to -1 and by $\operatorname{sgn} w$ the product of the ϵ_i's. We contend that $\operatorname{sgn} w$ is equal to the determinant of w viewed as a linear transformation of V, and, in particular, does not depend on $\mathcal{S}$. In fact, let e_i, e_{-i} be the orthonormal base of $\mathfrak{a}_i$ with respect to which we have (3) of § 1, and let $g \in N_T$ belong to the coset of w. It follows from 2.2 that w permutes the $\mathfrak{a}_i$, and then from (1) § 1 that if $w(a_i) = \epsilon_i a_j$, then $\operatorname{Ad} g(e_i \wedge e_{-i}) = \epsilon_i e_j \wedge e_{-j}$; moreover, the natural isomorphism of $\mathfrak{t}$ on V carries the restriction of $\operatorname{Ad} g$ to $\mathfrak{t}$ over to w; our contention follows readily from this and from the fact that, G being connected, we have $\det \operatorname{Ad} g = 1$.

2.7. *The Weyl chambers.* Let $a_1, \cdots, a_r$ be the simple roots belonging to the order $\mathcal{S}$. A *Weyl chamber* in V or V^* is a connected component of the set of regular elements. In particular, the set of points $v \in V$ (resp. $x \in V^*$), such that $a_i(v) > 0$, (resp. $(x, a_i) > 0$) $(1 \leqq i \leqq r)$, is one and will be called the positive Weyl chamber with respect to $\mathcal{S}$. The Weyl group acts simply transitively on the Weyl chambers, and, in particular, the integer $s(w)$ defined in 2.6 is zero if and only if w is the identity; it is generated by the symmetries to the hyperplanes $a_i = 0$ $(1 \leqq i \leqq r)$.

2.8. *Remark on orderings.* Let $a \in V^*$ be such that $(a, a_i) \neq 0$ for all i $(1 \leqq i \leqq m)$, and let us say that a root is positive if $(a, a_i) > 0$. Then the order relation thus obtained between roots is induced by an ordering on V^* as considered in (2.4) and has, therefore, the properties (2.4), (2.5). To define $\mathcal{S}$, one takes a base (x^i) of V^* dual to a base (e_i) $(1 \leqq i \leqq l)$, of V where e_i $(i \geqq 2)$ is contained in the hyperplane $a = 0$.

2.9. *Classification.* We recall that a compact connected Lie group G has a finite covering $\bar{G}$ which is the direct product of a torus S by a semi-simple and simply connected group $\bar{G}'$; the group $\bar{G}$ is uniquely determined, up to an isomorphism, if we require, moreover, that the kernel of the projection of $\bar{G}$ onto G intersects S only at the identity. The image of $\bar{G}'$ in G is the derived group G' of G and is also its largest semi-simple subgroup; the image of S is, of course, the connected identity component of the center of G.

The semi-simple groups are locally isomorphic to products of simple non-commutative groups. For the classification of the Lie algebras of compact simple Lie groups, we refer to [13, 23]. For a list of their roots, see for instance [25a]. For the simple Lie groups and the classical linear groups we follow here the standard notations.

3. Linear representations. a_i $(1 \leqq i \leqq m)$ are the positive roots of the compact connected Lie group G of rank l, with respect to an ordering $\mathcal{S}$, a is the sum of the a_i's and $a_1, \cdots, a_r$ are the simple roots, r being the rank of the semi-simple part G' of G.

3.1. LEMMA. *We have* $(a, a_j) = (a_j, a_j)$, $(1 \leqq j \leqq r)$.

Let S_j be the symmetry with respect to $a_j = 0$. We have

$$S_j a_i = a_i - 2(a_i, a_j) \cdot (a_j, a_j)^{-1} \cdot a_j.$$

Hence $S_j a_i$ and a_i $(j \leqq r)$, when expressed as linear combinations of simple roots, differ at most by the coefficient of a_j; thus, if $a_i \neq a_j$, $S_j a_i$ has at least one positive coefficient, and is a positive root by (2.4); this means that S_j permutes among themselves the positive roots different from a_j. But we have

$$(a_j, S_j a_i + a_i) = 0,$$

whence the lemma.

3.2. To abbreviate, we write $E(b)$, ($b \in V^*$ or $b \in V^* \otimes \boldsymbol{C}$), for

$$\sum_{w \in W(G)} (\operatorname{sgn} w) \exp(2\pi\sqrt{-1} \cdot w(b))$$

and $E(b, x)$ for the value of this function on $x \in V$. If b^* and x_* are the images of b and x under the canonical isomorphism between V and V^* defined by a metric invariant under $W(G)$, we have clearly $E(x_*, b^*) = E(b, x)$.

By a standard result of representation theory, we have

$$E(a/2) = \prod_{i=1}^{i=m} 2\sqrt{-1} \sin \pi a_i. \tag{1}$$

The computation of the m-th orders terms on each side yields the equality

$$m! \prod a_i = \sum_{w \in W(G)} (\operatorname{sgn} w) \cdot w(a/2)^m. \tag{2}$$

Let us denote by $E_x^{(m)}(b, 0)$ the value at 0 of the m-th derivative of $E(b, y)$ in the direction x; then we have

$$E_x^{(m)}(a/2, 0) = m!(2\pi\sqrt{-1})^m \prod_1^m \langle a_i, x\rangle. \tag{3}$$

It follows directly from the definition that $E(b)$ vanishes identically when b is singular. Conversely, the equality $E(x_*, b^*) = E(b, x)$, recalled above, and (3) imply

$$E_{a^*/2}{}^{(m)}(b, 0) = m!(2\pi\sqrt{-1})^m \prod_1^m \langle a_i, b\rangle = m!(2\pi\sqrt{-1})^m \prod_1^m (a_i, b)\,; \tag{4}$$

hence, if $E(b) = 0$, the element b must be singular.

3.3. *The weights.* An element $b \in V^*$ is called a weight of G if it is integral on the unit lattice of the connected identity component of the center of G and is such that $2(b, a_j) \cdot (a_j, a_j)^{-1}$ is an integer ($j \leqq m$). The weights form a free commutative group of rank l. The previous condition may also be expressed by saying that a weight is a linear form which is integral on the unit lattice Γ_0 corresponding to the covering $\bar{G}$ of G which has the form $S \times \bar{G}'$ where S is a torus, $\bar{G}'$ is semi-simple and simply connected, and such that the kernel of the projection $\bar{G} \to G$ intersects S only at the identity (2.9).

For $b, c \in V^*$, let us put $q(b, c) = 2 \cdot (b, c)(c, c)^{-1}$. Let S_d be the symmetry to the hyperplane $d=0$. We have $(b, S_d c)=(S_d b, c)$, $(S_d c, S_d c) = (c, c)$ and $S_d b = b - q(b, d)d$, and therefore

$$q(b, S_d c) = q(b, c) - q(b, d)q(d, c). \tag{5}$$

PROPOSITION. *Let b be an element of V^*. Then $q(b, a_j)$ is an integer for $1 \leqq j \leqq m$ if and only if it is so for $1 \leqq j \leqq r$. In particular, $a/2$ is a weight.*

The Weyl group $W(G)$ is generated by the symmetries S_j to the hyperplanes $a_j = 0$ $(1 \leqq j \leqq r)$, and every root is the image of a simple root under some transformation of $W(G)$ (this follows from 2.7). Since $q(d, c)$ is an integer when c and d are roots (2.3), the equality (5) shows that $q(b, S_j a_k)$ is integral if $q(b, a_k)$ and $q(b, a_j)$ are, and our first assertion follows by an obvious induction. The second one is then a consequence of (3.1) and of the fact that a is zero on the identity component of the center of G.

3.4. *Characters.* It follows from the results of H. Weyl and from standard facts about direct products, that the characters of the irreducible representations of the group $\bar{G}$ introduced in 3.3, restricted to the maximal torus $\bar{T}$, are the functions

$$\chi(t) = E(b) \cdot E(a/2)^{-1}, \tag{6}$$

where b runs through the weights contained in the positive Weyl chamber defined by $\mathcal{S}$. In other words, the b's are the weights which verify

$$2(a_j, b) = k_j(a_j, a_j), \qquad (k_j > 0, \text{ integral}, j = 1, \cdots, r).$$

By dividing out in (6), one may write $\chi(t)$ as a finite sum of exponentials $\exp 2\pi\sqrt{-1}\, c_s$, where the c_s's are weights. The highest one is $b - (a/2)$; it has multiplicity one and characterizes the linear representations up to an equivalence. In view of the foregoing, the highest weights are those which satisfy

$$2(a_j, c) = k_j(a_j, a_j), \qquad (k_j \geqq 0, \text{integral}, j = 1, \cdots, r). \tag{7}$$

Assume now G to be semi-simple, hence $r = l = \operatorname{rank} G$. Let ϖ_i be the linear form defined by $q(\varpi_i, a_j) = \delta_{ij}$ $(i = 1, \cdots, l)$. By (3.3), the ϖ_i's are weights, to be called the fundamental weights, and form a basis of the group of weights. By (7), the highest weights are the linear combinations of the ϖ_i's with integral non negative coefficients.

Let again $\bar{G}$ be compact, not necessarily semi-simple. The degree d of the representation with highest weight $b-(a/2)$ is $\chi(0)$. In the right hand side of (6), this appears in the form $0/0$, but by taking suitable m-derivatives at the origin, and using (2), (3), (4), one arrives easily at the formulas:

$$(8)\qquad \begin{aligned} d\cdot(m!)\cdot\prod_1^m a_i &= \sum_{w\in W(G)}(\operatorname{sgn} w)w(b)^m \\ d &= \prod_1^m (a_i,b)\cdot(a_i,a/2)^{-1}. \end{aligned}$$

Finally, we remark that the representation of $\tilde{G}$ with highest weight $b-(a/2)$ is single-valued on G if and only if $b-(a/2)$ is integral on the unit lattice corresponding to G.

4. Two characterizations of systems of positive roots. We assume here G to be semi-simple, and denote its rank by l, but otherwise follow the notations of § 3. We discuss here two conditions under which given roots are positive relative to a suitable ordering; the first one is the object of (4.3), which will be preceded by two lemmas.

4.1. LEMMA. *Let u_j be the integers such that the sum a of the positive roots is equal to $u_1a_1+\cdots+u_la_l$. Then the only solution of the system of inequalities*

$$(1)\quad (a_j,x)\geqq(a_j,a_j)\,;\ 0\leqq x_j\leqq u_j,\quad (x=x_1a_1+\cdots+x_la_l;\, j=1,\cdots,l),$$

is a itself.

That a is a solution follows from (3.1).

Let $y=y_1a_1+\cdots+y_la_l$ be a solution of (1) for which the sum of the y_i is minimum; such a y clearly exists. The y_i's are >0, because if, e.g., $y_k=0$, then we would have $(a_k,y)\leqq 0$ by (2.4).

Put $r_j=(a_j,y)$. Since the a_j's $(1\leqq j\leqq l)$ form a base, it is enough to show that $r_j=(a_j,a_j)$. Suppose otherwise; then there exists a k such that $r_k>(a_k,a_k)$. Consider $z=y-c\cdot a_k$, where c is a small positive constant. Then

$$z=\sum z_ja_j,\quad (z_j=y_j,\ (j\neq k)\,;\, z_k=y_k-c)$$
$$(a_j,z)=(a_j,y)-c(a_j,a_k)=r_j-(a_j,a_k)c.$$

Since $(a_j,a_k)\leqq 0$ for $j\neq k$ by (2.4), z is, for suitably small $c>0$, a solution of (1) for which the sum of the coefficients is strictly smaller than for y, contradicting the latter's definition.

4.2. LEMMA. *Let (ϵ_i), $(i=1,\cdots,m)$, be a sequence of integers of* *absolute value* 1, *and let* $a^* = \sum_i \epsilon_i a_i$. *If* $(a^*, a_j) > 0$ *for* $j = 1, \cdots, l$, *then* $a^* = a$ *and* $\epsilon_i = 1$ $(1 \leqq i \leqq m)$.

Let $c = c_1 a_1 + \cdots + c_l a_l$ (resp. $d = d_1 a_1 + \cdots + d_l a_l$), be the sum of the a_i for which $\epsilon_i = 1$ (resp. $\epsilon_i = -1$). We have

$$(2) \quad a^* = c - d;\ a = c + d;\ c_j + d_j = u_j;\ c_j, d_j \geqq 0, \qquad (j = 1, \cdots, l).$$

By assumption,

$$(a_j, c) - (a_j, d) = (a_j, a^*) > 0, \qquad (j = 1, \cdots, l),$$

and by (3.1),

$$(a_j, c) + (a_j, d) = (a_j, a) = (a_j, a_j), \qquad (j = 1, \cdots, l),$$

whence

$$2(a_j, c) > (a_j, a_j), \qquad (j = 1, \cdots, l).$$

But it follows from (2.3) that $2(a_j, c) \cdot (a_j, a_j)^{-1}$ is an integer; therefore the preceding inequality implies that

$$(a_j, c) \geqq (a_j, a_j), \qquad (j = 1, \cdots, l),$$

which, together with (2), shows that c is a solution of (1). By (4.1), this gives $c = a$, $d = 0$, $a = a^*$ and $d = 0$ implies (2.4) that no ϵ_i equals -1.

4.3. THEOREM. *Let* (ϵ_i), $(i = 1, \cdots, m)$, *be a sequence of integers of absolute value* 1. *Then the set* $(\epsilon_i a_i)$ *is the system of positive roots with respect to some ordering* $\mathcal{S}'$ *if and only if* $a^* = \sum_i \epsilon_i a_i$ *is a regular element.*

Necessity: Suppose that $(\epsilon_i a_i)$ are the positive roots with respect to some ordering; by (2.7), there exists $w \in W(G)$ which sends the $\epsilon_i a_i$ onto the a_i and, therefore, a^* onto a. Since the Weyl group leaves the set of regular elements invariant, it suffices to show that a is regular; but this follows from (3.1).

Sufficiency: Suppose a^* to be regular, and let $\mu_i = \pm 1$ be such that $(a^*, \mu_i a_i) > 0$. Then, as remarked in (2.8), $(\mu_i a_i)$ is the system of positive roots with respect to some ordering $\mathcal{S}_1$, and it will therefore be enough to show that $\mu_i = \epsilon_i$, $(i = 1, \cdots, m)$.

By (2.7), we may find $w \in W(G)$ carrying $(\mu_i a_i)$ onto (a_i) and, therefore, a^* onto $a^{**} = \sum_i \epsilon_i \mu_i a_{\sigma(i)}$, where σ is a permutation of $(1, 2, \cdots, m)$ since $(a^*, \mu_i a_i) > 0$ for all i and since w preserves the scalar product, we have

$(a^{**}, a_j) > 0$, $(j = 1, \cdots, l)$, and (4.2) gives then $a^{**} = a$ and $\mu_i \epsilon_i = 1$, $(i = 1, \cdots, m)$.

4.4. COROLLARY. *Let J be a non-empty set of integers belonging to the interval $[1, m]$. Suppose we have signs ϵ_j, $(j \in J)$, such that $\sum_{j \in J} \epsilon_j a_j = 0$. Then for any choice of the remaining signs ϵ_i, the form $\sum_1^m \epsilon_i a_i$ is a singular element.*

Suppose otherwise; then by (4.3), the $(\epsilon_i a_i)$ are the positive roots in some suitable ordering, but, obviously, a sum of positive roots cannot vanish.

4.5. DEFINITION. *A set B of roots of G is said to be closed if it contains the sum of any two of its elements whenever this sum is a root of G.*

Our main purpose will be to show that a closed system containing one root from each pair $\pm a_i$ is positive for some ordering.

4.6. LEMMA. *Let B be a closed system which for no i $(1 \leqq i \leqq m)$, contains both a_i and $-a_i$. Then if a linear combination b of elements of B with positive integral coefficients is a root, it belongs to B.*

Proof by induction on the sum k of the coefficients of b. For $k = 2$, it is an assumption; assume the lemma to be true for $k - 1$, and let

$$b = c_1 b_1 + \cdots + c_q b_q, \quad (c_i > 0, c_i \text{ integer}, \sum c_i = k, b_i \in B).$$

We distinguish two cases. (a) For some $j \leqq q$, $b_1 + b_j$ is a root; it is then in B by definition, and we have

$$b = (b_1 + b_j) + (c_1 - 1) b_1 + c_2 b_2 + \cdots + (c_j - 1) b_j + c_{j+1} b_{j+1} + \cdots + c_q b_q.$$

Therefore, b may also be written as

$$b = c'_1 b'_1 + \cdots + c'_r b'_r, \quad (c'_i > 0, \text{ integral}, \sum c'_i = k - 1, b'_i \in B),$$

and is in B by the induction assumption. (b) No element $b_1 + b_j$ is a root; then $(b_1, b_j) \geqq 0$ for $j = 2, \cdots, q$, (see 2.3), whence $(b_1, b) > 0$, and $b - b_1$ is a root. By induction, it is in B, and b then belongs to B by definition.

4.7. LEMMA. *We keep the same assumption on B. Then any sum $\sum c_i b_i$ $(b_i \in B, c_i > 0, \text{integral})$ is $\neq 0$.*

Otherwise, we would have

$$-b_1 = (c_1 - 1)b_1 + c_2b_2 + \cdots + c_qb_q,$$

contradicting (4.5) and (4.6).

4.8. A sequence $(b_1, \cdots, b_k)$ of elements of B such that $b_i - b_{i+1} \in B$ for $i = 1, \cdots, k-1$ will be said to be decreasing of length k. The height $h(b)$ of $b \in B$ will be the maximal length of decreasing sequences starting with b. By Lemma 4.7, any two elements in a decreasing sequence are different, and hence $h(b)$ is always finite. Let $k = h(b)$ and $b, b_2, \cdots, b_k$ a decreasing sequence. If we add to b a decreasing sequence for b_2 or for $b - b_2$, we clearly get a decreasing sequence starting with b. Therefore $h(b) = k$ implies that $h(b_2)$, $h(b - b_2)$ are $\leqq k - 1$; thus *an element of height* $k \geqq 2$ *is sum of two elements of heights* $\leqq k - 1$.

4.9. THEOREM. *Let B be a closed system of roots which, for each i, $(1 \leqq i \leqq m)$, contains exactly one of the two roots $\pm a_i$. Then B is the set of positive roots for a suitable ordering.*

Let $b_1, \cdots, b_s$ be the elements of height 1 in B. By induction on the height, it follows from the last assertion in (4.8) that every element of B is a linear combination of the b_i's $(i = 1, \cdots, s)$ with positive integral coefficients. Therefore, it suffices to show that the b_i's are linearly independent. Since they span all roots, their rank is l; assume that $b_1, \cdots, b_l$ are independent and that, contrary to our contention, $s \neq l$. We have then a relation

$$(3) \qquad b_{l+1} = c_1b_1 + \cdots + c_lb_l, \quad (c_i \text{ real, not all zero}).$$

The c_i's are also a solution of the linear system

$$(4) \qquad (x_1(b_1, b_j) + \cdots + x_l(b_l, b_j))(b_j, b_j)^{-1} = (b_{l+1}, b_j)(b_j, b_j)^{-1}$$

$(j = 1, \cdots, l)$, whose determinant is, up to a positive factor, the determinant of the products (b_i, b_j) and is therefore $\neq 0$. Thus the c_i's are the unique solution of (4) and are rational numbers since the coefficients are rational by (2.3). The given relation is then equivalent to a relation

$$d_1b_1 + \cdots + d_lb_l + d_{l+1}b_{l+1} = 0 \quad (d_i \text{ integers, } d_{l+1} \neq 0).$$

By (4.7) the coefficients do not all have the same sign, and, after a change in numeration of the b_i $(i \leqq l)$, we arrive at an equality

$$(5) \qquad e_1b_1 + \cdot\cdot\cdot + e_pb_p = e_{p+1}b_{p+1} + \cdot\cdot\cdot, + e_{l+1}b_{l+1} = b$$

($e_i \geqq 0$, integral, $(e_1, \cdot\cdot\cdot, e_p) \neq (0, \cdot\cdot\cdot, 0)$). On the other hand, we have $(b_i, b_j) \leqq 0$ for $(1 \leqq i < j \leqq s)$; because otherwise, by (2.3), the elements $\pm (b_i - b_j)$ would be roots, one of them would belong to B and either b_i or b_j would have a height $\geqq 2$. Therefore we have

$$(b, b) = (e_1b_1 + \cdot\cdot\cdot + e_pb_p, e_{p+1}b_{p+1} + \cdot\cdot\cdot + e_{l+1}b_{l+1}) \leqq 0$$

and $b = 0$, in contradiction to (4.7), which proves that $l = s$.

4.10. COROLLARY. *Let B be a closed system of roots which for each i, $(1 \leqq i \leqq m)$, contains at least one of the roots $\pm a_i$. Then B contains the set of all positive roots relative to a suitable ordering.*[4]

Let us number the roots in such a way that B consists of $\pm a_1, \cdot\cdot\cdot, \pm a_q$, $\epsilon_{q+1}a_{q+1}, \cdot\cdot\cdot, \epsilon_m a_m$ $(\epsilon_i = \pm 1)$. Then the system B' consisting of the a_i $(1 \leqq i \leqq q)$ and the $\epsilon_j a_j$ $(q < j \leqq m)$ is closed; in fact, if $a_s + a_t$ $(s, t \leqq q)$ is a root, it is positive and in B, hence in B'. If $a_s + \epsilon_t a_t = -a_p$ $(s, p \leqq q < t)$, then $a_s + a_p = -\epsilon_t a_t$ and B would not be closed; if $\epsilon_s a_s + \epsilon_t a_t = -a_p$, $(p \leqq q < s, t)$, then $a_p + \epsilon_t a_t = -\epsilon_s a_s$ and B is again not closed. Therefore, by the theorem, B' is the set of positive roots for some ordering.

4.11. *Remark.* Using complex semi-simple Lie algebras, one can also prove more generally than 4.9 that a closed system of roots B which for each i contains at most one of the roots $\pm a_i$ is positive for some ordering. In fact, in the notations of (12.2), it follows readily from (4.7) that the subspace of $\mathfrak{g}^c$ spanned by $\mathfrak{t}^c$ and the $\mathfrak{v}_b$, $(b \in B)$, is a solvable subalgebra. It is then conjugate by an inner automorphism α to a subalgebra of the algebra spanned by $\mathfrak{t}^c$ and the $\mathfrak{v}_{a_i}$ by a result of Morosow (C. R. Acad. Sci. U. R. S. S. (N. S.), 36 (1942), pp. 83-86), also proved in A. Borel, Annals of Math., 64 (1956), pp. 20-80, § 16. Moreover, by the conjugacy of Cartan subalgebras in solvable Lie algebras, we may assume that $\alpha(\mathfrak{t}^c) = \mathfrak{t}^c$ which means that B is transformed onto a subset of the a_i's by an element of the Weyl group.

5. The 2-roots of a compact Lie group. We define here certain linear forms with values in $\boldsymbol{Z}_2$, analogous to the roots, which are useful in the study of Stiefel-Whitney classes.

5.1. Let G be a Lie group. We denote by Q or Q_s a subgroup of G

---

[4] Another, completely different, proof of this corollary has been given by Harish-Chandra, *American Journal of Mathematics*, vol. 77 (1955), pp. 743-777, § 2, Lemma 4.

isomorphic to the product of s copies of $\boldsymbol{Z}_2$. The real irreducible linear representations of Q are 1-dimensional, being defined by a character which may be viewed as an element of $\mathrm{Hom}(Q, \boldsymbol{Z}_2)$. Let us now decompose the Lie algebra $\mathfrak{g}$ of G into a direct sum

$$\mathfrak{g} = \mathfrak{b}_1 + \cdots + \mathfrak{b}_n, \qquad (n = \dim \mathfrak{g})$$

of 1-dimensional subspaces invariant under $\mathrm{Ad}_{\mathfrak{g}} Q$; the characters $b_1, \cdots, b_n$ corresponding to these subspaces will be called the *2-roots of G with respect to Q*. In case Q is contained in a maximal torus, these are just the restrictions to Q of the roots of G and the zero form with multiplicity $l = \mathrm{rank}\,(G)$, but otherwise, they represent different elements of the group-theoretical structure of G and have a "global" character.

5.2. Let U be a closed subgroup of G containing Q. Then we can choose a decomposition into subspaces $\mathfrak{b}_i$, such that the $n-k$ last ones generate the Lie algebra $\mathfrak{u}$ of U. The 2-roots b_i $(1 \leqq i \leqq k)$ are then the *complementary* 2-roots; or, more explicitly, the 2-roots of G with respect to Q which are complementary to those of U.

Examples.

5.3. $G = \boldsymbol{O}(n)$, $\boldsymbol{SO}(n)$. We consider in $\boldsymbol{O}(n)$ the subgroup $\boldsymbol{Q}$ of diagonal matrices; it is a maximal commutative subgroup of type $(2, 2, \cdots, 2)$, and any subgroup of this type is conjugate to a subgroup of $\boldsymbol{Q}$. We take in $\mathfrak{g}$ the usual basis consisting of the antisymmetric matrices having only two non-vanishing entries, equal to ± 1. Let x_{i1} $(1 \leqq i \leqq n)$ be the diagonal matrix all of whose coefficients are equal to 1, except for the i-th one which is equal to -1, and let (y_i) be the dual basis of $\mathrm{Hom}(\boldsymbol{Q}, \boldsymbol{Z}_2)$. A straightforward computation shows that the basis of $\mathfrak{g}$ mentioned above is invariant under $\mathrm{Ad}_{\mathfrak{g}} \boldsymbol{Q}$ and that the 2-roots relative to $\boldsymbol{Q}$ are

$$y_i - y_j, \qquad (1 \leqq i < j \leqq n).$$

In $\boldsymbol{SO}(n)$, the diagonal matrices also form a maximal commutative subgroup $\boldsymbol{Q}'$ of type $(2, 2, \cdots, 2)$, isomorphic to $(\boldsymbol{Z}_2)^{n-1}$. It is convenient to consider it as a subgroup of $\boldsymbol{Q}$, and, therefore, $\mathrm{Hom}(\boldsymbol{Q}', \boldsymbol{Z}_2)$ as a quotient of $\mathrm{Hom}(\boldsymbol{Q}, \boldsymbol{Z}_2)$; it is then generated by n elements y_i subject to the relation $y_1 + \cdots + y_n = 0$, and the 2-roots are again the differences $y_i - y_j$ $(1 \leqq i < j \leqq n)$.

5.4. $G = \boldsymbol{U}(n), \boldsymbol{SU}(n)$. In $\boldsymbol{U}(n)$, all maximal commutative subgroups of type $(2, 2, \cdots, 2)$ are conjugate to the subgroup $\boldsymbol{Q}$ of diagonal matrices with coefficients ± 1, and are therefore contained in maximal tori. The 2-roots are then obtained from the usual roots and, with respect to the standard basis of skew-hermitian matrices, are the zero form with multiplicity n and the differences $y_i - y_j$ $(1 \leqq i < j \leqq n)$, each with multiplicity two.

The 2-roots of $\boldsymbol{SU}(n)$ with respect to the subgroup of the elements of $\boldsymbol{Q}$ having determinant 1 will be the same, the y_i's being subject to the relation $y_1 + \cdots + y_n = 0$, the zero form having multiplicity $n-1$.

5.5. $G = \boldsymbol{Sp}(n)$. Here again, all maximal commutative subgroups of type $(2, 2, \cdots, 2)$ are conjugate to the subgroup $\boldsymbol{Q}$ of diagonal matrices with coefficients ± 1 (G being considered as the group of unitary matrices with quaternionic coefficients) and are isomorphic to $(\boldsymbol{Z}_2)^n$. Since the usual roots are $\pm y_i \pm y_j$ $(1 \leqq i < j \leqq n)$ and $\pm 2y_i$ $(1 \leqq i \leqq n)$, we get as 2-roots: the root zero, with multiplicity $3n$ and $y_i - y_j$ $(1 \leqq i < j \leqq n)$, with multiplicity 4.

In § 17, we shall also discuss the 2-roots of the exceptional group $\boldsymbol{G}_2$ with respect to a subgroup not contained in a maximal torus.

Chapter II. Topological Preliminaries.

6. Fibre bundles.

6.1. *Notations.* p denotes a prime number or zero, K_p a field of characteristic p, $\boldsymbol{Z}_p$ $(p \neq 0)$, $\boldsymbol{Z}_0$, $\boldsymbol{R}$, $\boldsymbol{C}$, the fields of integers mod p, of rational, real, complex numbers respectively.

$H^i(X, A)$ (resp. $H_i(X, A)$) is the i-th singular cohomology (resp. homology) group of the space X with coefficients in the commutative group A, $H^*(X, A)$ (resp. $H_*(X, A)$) the direct sum of the cohomology (resp. homology) groups; for all spaces considered in this paper, $H^i(X, \boldsymbol{Z})$ will be finitely generated and equal to the i-th Alexander-Spanier cohomology group. The map of cohomology (resp. homology) groups induced by a continuous map f is denoted by f^* (resp. f_*).

When dealing with classifying spaces, it will sometimes be convenient to consider formal infinite sums of cohomology elements, and to this effect, we also introduce the *direct product* $H^{**}(X, A)$ of the $H^i(X, A)$; an element $x \in H^{**}(X, A)$ may be identified with a sum $x_0 + \cdots + x_i + \cdots$, with $x_i \in H^i(X, A)$ possibly $\neq 0$ for infinitely many values of i. When A is a ring, $H^{**}(X, A)$ also becomes an associative ring under the cup product. The homomorphism of $H^{**}(Y, A)$ into $H^{**}(X, A)$ induced by $f: X \rightarrow Y$ will be denoted by f^{**}.

$A\{X_1,\cdots,X_k\}$ will denote the ring of formal power series in the X_i's, with coefficients in the commutative ring A.

Let U be a closed, connected subgroup of maximal rank of the compact, connected Lie group G, and let T be a maximal torus of U. We have then $H^{**}(B_T,A)=A\{x_1,\cdots,x_l\}$, $(x_i\in H^2(B_T,A),\ 1\leqq i\leqq l=\operatorname{rank} G)$. The results of [2, §§ 26, 27] imply that $\rho^{**}(T,G)$ maps $H^{**}(B_G,\boldsymbol{Z}_0)$ isomorphically onto the ring of invariants of the Weyl group, and that it is isomorphic to a ring of formal power series in l indeterminates; moreover, $H^{**}(G/U,\boldsymbol{Z}_0)$ is the quotient of $H^{**}(B_U,\boldsymbol{Z}_0)$, regarded as a subring of $H^{**}(B_T,\boldsymbol{Z}_0)$, by the ideal $(I^+_G)^*$ generated in $H^{**}(B_U,\boldsymbol{Z}_0)$ by the (finite or infinite) sums of homogeneous invariants of $W(G)$ with strictly positive degrees. Similar translations in cohomology over $\boldsymbol{R}$, $\boldsymbol{Z}_p$ or $\boldsymbol{Z}$ of the results of [2, § 29] are left to the reader.

6.2. *Fibre bundles.* The fibre bundles occurring in this paper will be locally trivial; we follow the definitions of [19, 26]. We do not require the structural group to act effectively on the fibre [19, § 3.2c)]. A fibre bundle is denoted by (E,B,F,π) or (E,B,F), where E is the total space, B the base space, F the typical fibre, π the propection, or just by one symbol, mostly ξ, η, θ; in the latter case, we often write $E_\xi, B_\xi, F_\xi, \pi_\xi$, G_ξ, τ_ξ for E, B, F, π, the structural group and the transgression in ξ respectively. A bundle with structural group G will also be called a G-bundle.

Let ξ be a principal G-bundle and U a closed subgroup of G. The space of the cosets $x\cdot U$ modulo U $(x\in E_\xi)$, is denoted by E_ξ/U; it is the base space of the principal fibering $(E_\xi, E_\xi/U, U)$ and the total space of the G-bundle $(E_\xi/U, B_\xi, G/U)$. Let F be a space operated upon by G. We denote by $E_\xi\times_G F$ the quotient of $E_\xi\times F$ by the equivalence relation $(x,f)\approx(x\cdot g, g^{-1}\cdot f)$. As is well known, it is the total space of a G-bundle (ξ,F) over B_ξ, with fibre F.

6.3. *Representations of fibre bundles.* Let ξ,η be two fibre bundles. A representation of ξ in η is a continuous map $\phi\colon E_\xi\to E_\eta$ which sends fibres into fibres; it induces then a map $\bar\phi\colon B_\xi\to B_\eta$ such that $\bar\phi\circ\pi_\xi=\pi_\eta\circ\phi$. We shall use without further comment the fact that ϕ commutes with transgression and, more generally, induces a homomorphism of the spectral sequence of η into that of ξ (see e.g. [2], § 4).

6.4. *Homomorphisms of fibre bundles.* Let G, G' be topological groups, $\lambda\colon G\to G'$ a homomorphism, and F (resp. F'), a space on which G, (resp. G'), operates. A λ-map of F into F' is a continuous map ψ such that

$\psi(g\cdot f)=\lambda(g)\cdot\psi(f)$, (or $\psi(f\cdot g)=\psi(f)\cdot\lambda(g)$ if G, G' operate on the right). Let ξ and η be principal G- and G'-bundles respectively. A homomorphism of ξ into η is a representation induced by a λ-map of E_ξ into E_η; clearly every λ-map defines a homomorphism. A homomorphism of (ξ, F) into (η, F') is a representation defined by two λ-maps of E_ξ and F into E_η and F' respectively.

Let U, U' be closed subgroups of G and G' such that $\lambda(U)\subset U'$. Then we have a commutative diagram

$$\begin{tikzcd}
E_\xi \arrow[r] \arrow[d, "\phi"] & E_\xi/U \arrow[r] \arrow[d, "\phi_1"] & B_\xi \arrow[d, "\phi_2"] \\
E_\eta \arrow[r] & E_\eta/U' \arrow[r] & B_\eta
\end{tikzcd}$$

ϕ defines λ-homomorphisms $(E_\xi, E_\xi/U, U)\rightarrow(E_\eta, E_\eta/U', U')$ and $E_\xi, B_\xi, G)\rightarrow(E_\eta, B_\eta, G')$; the map ϕ_1 is a λ-homomorphism of $(E_\xi/U, B_\xi, G/U)$ into $(E_\eta/U', B_\eta, G'/U')$.

6.5. *Restriction and extension of the structural group.* Let ξ and η be two principal bundles over the same base space B, and let λ be a homomorphism of G_ξ into G_η. Assume that there exists a λ-homomorphism of ξ into η which induces the identity of B. Then we say that η is a λ-extension of ξ and that ξ is a λ-restriction of η. We recall that, given ξ and λ, there always exists a λ-extension which is unique up to equivalence, and which will be denoted by $\lambda(\xi)$; whereas given η and λ, a λ-restriction does not always exist and, if it does, is not necessarily unique. The λ-extension η of ξ is defined as follows: $E_\eta=E_\xi\times_G G'$, where G operates on G' by $g\cdot g'=\lambda(g)\cdot g'$; if μ is the projection of $E_\xi\times G'$ onto E_η, then π_η is induced by $\mu(x, g')\rightarrow\pi_\xi(x)$, and the λ-map $\phi: E_\xi\rightarrow E_\eta$ is defined by $\phi(x)=\mu(x,\epsilon)$, where e is the neutral element in G'; finally, the principal bundle operations on E_η are introduced by $(x,y)\cdot g'=(x, y\cdot g')$, $(x\in E_\xi; y, g'\in G')$. These notions are defined in the same way for associated bundles; they generalize the standard concepts of extension and restriction of the structural group, to which they reduce when λ is the inclusion map of a closed subgroup. Clearly they can also be formulated for equivalence classes of bundles; if these are identified with the elements of the cohomology sets $H^1(B, G_c)$ and $H^1(B, G'_c)$, in the notations of [19, § 3], then the λ-extension of $\xi\in H^1(B, G_c)$ is its image under the natural coefficient map induced by λ.

6.6. *Characteristic map.* E_G (resp. B_G) is a universal bundle (resp. classifying space) for the compact Lie group G ([26], § 19, [2], § 18; as in

[6] they will usually be taken as universal or classifying for all dimensions). Any principal G-bundle ξ over a base space B belonging to a suitable class of topological spaces is induced from the universal bundle by a map $\sigma : B \to B_G$, defined up to homotopy as the "characteristic map" for ξ [26, § 19].

To a homomorphism λ of G into a compact Lie group G' corresponds a map $\rho(\lambda)$ of B_G into $B_{G'}$, defined up to homotopy, called the characteristic map for the λ-extension of (E_G, B_G, G) (see [6], § 1). It follows immediately from the definitions that a λ-restriction of a principal G'-bundle η exists if and only if the characteristic map σ of η can be written as $\sigma = \rho(\lambda) \circ \sigma'$ where σ' is a map of B into B_G; when λ is an inclusion, $\rho(\lambda)$ reduces to the map $\rho(G, G')$ introduced in [2].

6.7. *Fibre bundle over a fibre bundle.* We discuss here a generalization of the "bundle along the fibres" (see § 7), which allows us to put in its proper setting a useful fact about characteristic maps.

Let ξ, η be fibre bundles, $\bar{\xi}$, $\bar{\eta}$ the corresponding principal bundles. We assume that $F_\xi = B_\eta$ and that G_ξ is also a group of automorphisms of $\bar{\eta}$; the latter condition means that there is a homomorphism $g \to \bar{g}$ of G_ξ in the group of those homeomorphisms of $E_{\bar{\eta}}$ which commute with the operations of G_η, and, of course, such that the induced homeomorphisms of B_η are those which define G_ξ as structural group for ξ. In particular, the homeomorphism $\bar{g} \times \mathrm{Id}$ of $E_{\bar{\eta}} \times F_\eta$ is compatible with the equivalence relation which defines η, hence G_ξ is also a group of homeomorphisms of E_η commuting with π_η. By means of these operations, we define first a bundle $\mu = (E_\mu, B_\xi, E_\eta)$ with structural group G_ξ, and typical fibre E_η, associated to $\bar{\xi}$; its total space is then

$$E_\mu = E_{\bar{\xi}} \times_{G_\xi} E_\eta.$$

Since G_ξ commutes with π_η, this map induces a map λ of E_μ onto $E_{\bar{\xi}} \times_{G_\xi} B_\eta = E_\xi$. Since G_ξ, operating on $E_{\bar{\eta}}$, and G_η commute, the space $E_{\bar{\xi}} \times_{G_\xi} E_{\bar{\eta}}$ can be considered as a principal G_η-bundle over E_ξ, the operations of the group being defined by means of its action on the right factor, and moreover, we have the "associativity law"

$$(E_{\bar{\xi}} \times_{G_\xi} E_{\bar{\eta}}) \times_{G_{\bar{\eta}}} F_\eta \approx E_{\bar{\xi}} \times_{G_\xi} (E_{\bar{\eta}} \times_{G_{\bar{\eta}}} F_\eta).$$

From this, it follows immediately that λ is the projection in a fibre bundle $(E_\mu, E_\xi, F_\eta) = \nu$, in which G_η is the structural group, and whose corresponding principle bundle has total space $E_{\bar{\xi}} \times_{G_\xi} E_{\bar{\eta}}$. Therefore, we have obtained a bundle over E_ξ with fibre F_η. It is clear that the inclusion map of a fibre of μ in E_μ may be viewed as a homomorphism of η in ν; it induces a map $i : B_\eta \to E_\xi$ of their base spaces which is the inclusion map of a fibre of ξ.

Therefore, if σ is the characteristic map for ν, then $\sigma\circ i$ is characteristic for η, and the characteristic ring of η is the image of $i^*\circ\sigma^*$. This proves in particular the following:

6.8. PROPOSITION. *Let* ξ, η *be two bundles with* $F_\xi = B_\eta$, *satisfying the conditions of* 6.7., *and let* i *be the injection of a fibre of* ξ. *Then the image of* $i^*: H^*(E_\xi, A) \to H^*(F_\xi, A)$ *contains the characteristic ring of* η.

Let G be a topological group, U be a closed subgroup and θ be a principal G-bundle. Then $\xi = (E_\theta/U, B_\theta, G/U)$ and $\eta = (G, G/U, U)$ satisfy the assumptions of 6.7, η being considered as a principal U-bundle, and $G_\xi = G$ (resp. $G_\eta = U$) acting by means of left (resp. right) translations on G; in this case, μ may be identified with θ and ν with $(E_\theta, E_\theta/U, U)$, and 6.8 reduces to the corollary to Prop. 18.3 of [2]. The application to differentiable bundles will be mentioned in § 7.

7. Vector bundles.

7.1. A real (resp. complex) vector bundle is a fibre bundle with an n-dimensional real (resp. complex) vector space as typical fibre, the structural group operating by means of linear transformations. Most often, we shall identify the typical fibre with $\boldsymbol{R}^n$ or $\boldsymbol{C}^n$, and the structural group with a subgroup of $\boldsymbol{GL}(n,\boldsymbol{R})$ or $\boldsymbol{LG}(n,\boldsymbol{C})$. We refer to [19] for the notions of sub-bundle, quotient bundle of a vector bundle, of Whitney sum $\xi\oplus\eta$ and tensor product $\xi\otimes\eta$ of two vector bundles ξ, η. We recall that a principal bundle with group $\boldsymbol{GL}(n,\boldsymbol{R})$ or $\boldsymbol{GL}(n,\boldsymbol{R})^+$ or $\boldsymbol{GL}(n,\boldsymbol{C})$ has a unique restriction (up to isomorphism) with group $\boldsymbol{O}(n)$ or $\boldsymbol{SO}(n)$ or $\boldsymbol{U}(n)$ [26, § 12].

7.2. *Orientable real vector bundles.* A real vector bundle is orientable if its structural group can be reduced to $\boldsymbol{GL}(n,\boldsymbol{R})^+$ or $\boldsymbol{SO}(n)$. If such a restriction has been made, we then endow each fibre with the orientation which is carried over from a fixed given orientation of the typical fibre V by the allowable homeomorphisms of the bundle structure; the bundle is then said to be oriented; if V has been identified with $\boldsymbol{R}^n$, we always take the natural orientation of $\boldsymbol{R}^n$.

7.3. *Almost complex structures.* A complex vector bundle $(E, B, \boldsymbol{C}^q)$ defines in a natural fashion a real vector bundle $(E', B, \boldsymbol{R}^{2q})$, its λ-extension relative to the standard inclusion $\lambda\colon \boldsymbol{GL}(q,\boldsymbol{C}) \to \boldsymbol{GL}(2q,\boldsymbol{R})$; it is oriented. Conversely, if a real vector bundle $(E, B, \boldsymbol{R}^{2q})$ has a λ-restriction, we say that it admits a complex structure and that such a complex restriction is a complex structure of the given bundle. A differentiable manifold admits an almost complex structure (resp. is almost complex) if its tangent bundle admits (resp. has been given) a complex structure.[5] To a complex structure of $\xi = (E, B, \boldsymbol{R}^{2n})$ there is attached a section J in the real vector bundle $\xi^* \otimes \xi = \operatorname{Hom}(\xi, \xi)$, where the value of J_b of J at $b \in B$ is the linear map defined by multiplication by $\sqrt{-1}$; conversely, given a section J of linear maps such that $J_b{}^2 = -\mathrm{Id}$ for all $b \in B$, we introduce on each fibre a complex structure by putting

$$(x + \sqrt{-1}\, y) \cdot v = x \cdot v + y \cdot J_b(v),$$

which gives a complex structure for the given real vector bundle.

7.4. *The bundle along the fibres.* Let ξ be a fibre bundle whose fibre is a differentiable manifold F of dimension n, G_ξ being a group of differentiable homeomorphisms of F; the group G_ξ is then also a group of automorphisms of the tangent bundle $\eta = T(F_\xi)$ to F_ξ and of the bundle of frames $\bar{\eta} = B(F_\xi)$ which have $\boldsymbol{GL}(n, \boldsymbol{R})$ as structural group. We may apply 6.7, and the bundle corresponding to ν of 6.7 will be called *the bundle along the fibres.* It is a real vector bundle over $\boldsymbol{E}_\xi$, whose fibres are the tangent spaces to the fibres of ξ, and will be denoted by $\hat{\xi}$. If F has an almost complex structure which is invariant under G_ξ, in other words, if G_ξ is also a group of automorphisms for a complex structure η' of η, then the construction of 6.7 may also be applied to ξ and η' and yields a complex structure on $\hat{\xi}$ which will then be called a *complex bundle along the fibres of* ξ. Also, if F_ξ carries an orientation invariant under G_ξ, then the structural group of $\hat{\xi}$ may also be reduced to $\boldsymbol{GL}(n, \boldsymbol{R})^+$. Applying 6.8 to the basic elements of the characteristic ring of a $\boldsymbol{O}(n)$, $\boldsymbol{SO}(n)$ or $\boldsymbol{U}(n)$-bundle (see § 9), we obtain the

PROPOSITION. *Let ξ be a fibre bundle whose typical fibre F_ξ has a differentiable structure invariant under G_ξ, and let i be the inclusion map of a fibre in E_ξ. Then the Pontrjagin and Stiefel-Whitney classes of F_ξ, its Euler-Poincaré class with respect to an orientation invariant under G_ξ, and its Chern classes with respect to a G_ξ-invariant almost complex structure are in the image of i^*.*

(A similar remark has already been made in A. Borel, Jour. math. pur. appl. (9) 35, 127-139 (1956), proof of 3.2.)

---

[5] In this terminology therefore, an *almost complex* structure on a manifold corresponds to a *complex* structure of its tangent bundle.

ξ is said to be differentiable if E_ξ, B_ξ, F_ξ are differentiable manifolds, π_ξ is a differentiable map, and the coordinate functions are differentiable; it follows then that G_ξ is a group of diffeomorphisms of F_ξ. In this case, the fibre of $\hat{\xi}$ over $x \in E_\xi$ may be identified with the subspace of the tangent space of E_ξ at x which is tangent to the fibre of ξ passing through x.

7.5. PROPOSITION. *Let G be a Lie group, U a closed subgroup, $\iota: U \to \boldsymbol{GL}(n, R)$ the isotropy representation* (1.1), *and let ξ be a principal G-bundle. Then the principal bundle η along the fibres of $(E_\xi/U, B_\xi, G/U)$ is the ι-extension of $(E_\xi, E_\xi/U, U)$.*

We have to show the existence of a ι-map: $E_\xi \to E_\eta$ inducing the identity on E_ξ/U.

We recall first that $(E_\xi/U, B_\xi, G/U)$ may be considered as the bundle with typical fibre G/U associated to ξ; more precisely, there is a commutative diagram

$$\begin{tikzcd}
E_\xi \arrow[r, "\alpha"] \arrow[d, "\gamma"] & E_\xi \times G/U \arrow[d, "\delta"] \\
E_\xi/U \arrow[r, "\beta"] & E_\xi \times_G G/U
\end{tikzcd}$$

where γ and δ are the natural projections, α is defined by $x \to (x, o)$, the point $o \in G/U$ being the image of U under the projection, β is determined by the other maps and is a homeomorphism. This also allows us to attach to each $x \in E_\xi$ a homeomorphism σ_x of G/U onto the fibre $\gamma(x \cdot G)$ of $\gamma(x)$ in E_ξ/U, defined by

$$\sigma_x(y) = \gamma \cdot \alpha^{-1}(x \cdot g, o), \quad (y \in G/U, \; g \in G \text{ such that } g^{-1}(y) = o).$$

We have

$$\sigma_x(o) = \gamma(x); \quad \sigma_{x \cdot g} = \sigma_x \circ g.$$

All this is well known and easily checked. Let now R_0 be a fixed base of the tangent space to G/U at o. Then $\sigma_x(R_0)$ is a base of the tangent space to the fibre of $(E_\xi/U, B_\xi, G/U)$ at $\gamma(x)$. We define ϕ by $\phi(x) = \sigma_x(R_0)$; from the relation $\sigma_{x \cdot u} = \sigma_x \circ u$, it follows readily that $\phi(x \cdot u) = \phi(x) \cdot \iota(u)$, in other words, that ϕ is a ι-map. Since by construction, ϕ induces the identity on E_ξ/U, our contention is proved.

(7.5) shows in particular that the structural group of the tangent bundle to G/U may be ι-restricted to U. Finally, we mention the following well known elementary fact:

7.6. PROPOSITION. *Let ξ be a differentiable bundle. Then the quotient of the tangent bundle to E_ξ by the bundle along the fibres $\hat{\xi}$ is equivalent to the bundle induced by π_ξ from the tangent bundle to B_ξ.*

In fact, π_ξ induces a bundle map of this quotient onto the tangent bundle to B_ξ, and the proposition follows then from [26, § 10.3].

8. Integration over the fibre.

8.1. Let A be a commutative group, (E, B, F, π) a fibre bundle with connected fibres such that (i) there exists an integer q for which $H^r(F, A) = 0$ for $r > q$ and that (ii) the cohomology groups of the different fibres form a constant sheaf over B.

We want to define, in terms of the spectral sequence of the bundle, a homomorphism

$$\natural\colon H^k(E, A) \rightarrow H^{k-q}(B, H^q(F, A)) \qquad (k = 0, 1, \cdots),$$

the so-called "integration over the fibre". We put, of course, $\natural = 0$ for $k < q$ and assume from now on that $k \geqq q$. By (i), no non-zero element of $E_r^{k-q,q}$, $(r \geqq 2)$, is a coboundary, hence the subgroup of the elements in $E_2^{k-q,q}$ which are cocycles for all differentials is canonically isomorphic to $E_\infty^{k-q,q}$, and we get a natural inclusion map

$$h_1\colon E_\infty^{k-q,q} \rightarrow E_2^{k-q,q} \cong H^{k-q}(B, H^q(F, A)).$$

Let now J^a $(a = 0, 1, \cdots)$, be the decreasing sequence of submodules defining the filtration of $H^*(E, A)$ attached to the fibration, and let us put, as usual, $J^{a,b} = J^a \cap H^{a+b}(E, A)$. Since $E_\infty^{a,b} = 0$ for $b > q$, we have $H^k(E, A) = J^{k-q,q}$, whence

$$E_\infty^{k-q,q} = J^{k-q,q}/J^{k-q+1,q-1} = H^k(E, A)/J^{k-q+1,q-1}$$

and a natural projection

$$h_2\colon H^k(E, A) \rightarrow E_\infty^{k-q,q}.$$

$\natural$ is then defined by $\natural = h_1 \circ h_2$; by linearity it extends to an additive homomorphism of $H^*(E, A)$ into $H^*(B, H^q(F, A))$ and of $H^{**}(E, A)$ into $H^{**}(B, H^q(F, A))$. Whenever $H^q(F, A)$ can be identified with A, for instance, when F is an oriented q-dimensional manifold, we consider it as a map from $H^*(E, A)$ or $H^{**}(E, A)$ to $H^*(B, A)$ or $H^{**}(B, A)$, lowering by q the degree of homogeneous elements.

8.2. PROPOSITION. *Let* A *be a commutative ring,* ξ *a bundle satisfying conditions* (i), (ii) *of* (8.1), $\natural$ *the integration over the fibre. Then*

$$(\pi_\xi^*(b)\cdot x)^\natural = b\cdot (x)^\natural, \quad (b \in H^*(B,A), x \in H^*(E,A)).$$

(Here $b\cdot(x)^\natural$ means the product of b and $(x)^\natural$ under the natural pairing of A and $H^q(F_\xi, A)$ to $H^q(F_\xi, A)$.) For the proof, we may assume b and x to be homogeneous of degrees s, t. We identify b with its image in $E_2^{s,0}$ under the canonical isomorphism with $H^s(B_\xi, H^0(F_\xi, A)) = H^s(B_\xi, A)$. Then we have

$$h_2(\pi_\xi^*(b)\cdot(x)) = \kappa_\infty^2(b)\cdot h_2(x)$$
$$h_1(\kappa_\infty^2(b)\cdot h_2(x)) = b\cdot(h_1\circ h_2(x))$$

because E_∞ is the graded ring associated to $H^*(E_\xi, A)$ filtered by the J^a, and b is a cocycle for all differentials.

8.3. PROPOSITION. *Let* ξ, η *be two fibre bundles satisfying the conditions* (i), (ii) *of* (8.1) *and let* ϕ *be a representation of* ξ *in* η. *Let* ψ: $H^*(B_\eta, H^q(F_\eta, A)) \to H^*(B_\xi, H^q(F_\xi, A))$ *be the homomorphism which is induced by the map* $\bar\phi: B_\xi \to B_\eta$ *defined by* ϕ, *and by the map* ν: $H^*(F_\eta, A) \to H^*(F_\xi, A)$ *defined by the restriction of* ϕ *to a fibre.*[6]. *Then the following diagram is commutative*

$$\begin{tikzcd}
H^k(E_\eta, A) \arrow[r, "\phi^*"] \arrow[d, "\natural"] & H^k(E_\xi, A) \arrow[d, "\natural"] \\
H^{k-q}(B_\eta, H^q(F_\eta, A)) \arrow[r, "\psi"] & H^{k-q}(B_\xi(H^q(F_\xi, A)).
\end{tikzcd}$$

This follows from the fact that ϕ induces a homomorphism of the spectral sequence of η into that of ξ, reducing to ψ on the E_2 terms [2, § 4].

Remark. For another discussion of the integration over the fibre, see [11]; it is also proved there, but we shall not need this fact, that in case E, B, F are oriented compact connected manifolds, then $\natural$ is equivalent to the Gysin homomorphism defined by means of π [11, Theorem 3].

8.4. Let ξ be a fibre bundle satisfying (i), (ii) and: (iii) A is a principal ideal ring, $H^*(F_\xi, A)$ is a free A-module of finite rank, $H^q(F_\xi, A) \cong A$, and F_ξ is totally non-homologous to zero in E_ξ.

As is well known, these conditions have the following consequences for the spectral sequence of ξ:

---

[6] Note that, by assumption (ii), the latter homomorphism has an invariant meaning, independent from the particular fibre to which we restrict ϕ.

$$E_\infty = E_2 = H^*(B_\xi, A) \otimes H^*(F_\xi, A),$$

and $\pi_\xi{}^*$ is injective; if $H^*(E_\xi, A)$ is considered as a $H^*(B_\xi, A)$-module by means of the rule $b \cdot x = \pi_\xi{}^*(b) \cup x$, $(b \in H^*(B_\xi, A),\ x \in H^*(E_\xi, A))$, and if h_i $(1 \leqq i \leqq m = \operatorname{rank} H^*(F_\xi, A))$ are homogeneous elements of $H^*(E_\xi, A)$ inducing a module basis of $H^*(F_\xi, A)$, then $H^*(E_\xi, A)$ is a free $H^*(B_\xi, A)$-module with base (h_i).

Assume that h_1 induces a generator $\bar{h}_1$ of $H^q(F_\xi, A)$, and use $\bar{h}_1$ to identify $H^q(F_\xi, A)$ with A. Then we have clearly

$$x = \pi_\xi{}^*(x^\natural) \cdot h_1 + \sum_2^m \pi_\xi{}^*(b_i) \cdot h_i, \tag{1}$$

and this characterizes $x^\natural$ completely.

Let μ, ν be two fibre bundles with the following properties: $E_\mu = E_\xi$, $B_\mu = E_\nu$, $B_\nu = B_\xi$, $\pi_\xi = \pi_\nu \circ \pi_\mu$, and the restriction of π_μ to a fibre of ξ is the projection map in a fibre bundle $\theta = (F_\xi, F_\nu, F_\mu)$. Assume that ξ, μ, ν, θ satisfy (i), (ii), (iii), (with of course q depending on the fibre bundle); let h_μ, h_ν be homogeneous elements of $H^*(E_\mu, A)$, $H^*(E_\nu, A)$ whose restrictions to a fibre generate the highest non-vanishing cohomology groups. Then $\pi_\mu{}^*(h_\nu) \cdot h_\mu = h_\xi$ has the same property in ξ. If these elements are used to identify the corresponding cohomology groups of the fibres with A, then it follows immediately from (1) that

$$\natural_\xi = \natural_\nu \circ \natural_\mu. \tag{2}$$

When ξ, μ, ν, θ are fibre bundles satisfying (i), (ii) whose total spaces, fibres and base spaces are compact oriented manifolds, then (2) follows directly from the equivalence with the Gysin homomorphism mentioned in 8.3; it was shown to us to be true in general by Puppe, but since this is not needed here, we shall not reproduce the somewhat longer proof of this fact.

Chapter III. Roots and Characteristic Classes.

9. Characteristic classes. We recall here the definitions of Chern, Stiefel-Whitney and Pontrjagin classes to be used in this paper, i. e., mainly the definitions which use universal bundles and flag manifolds. $S(x_1, \cdots, x_n)$ is the ring of symmetric polynomials in the x_i's, with respect to a ring of coefficients which the context will make precise. $S\{x_1, \cdots, x_n\}$ is the corresponding ring of symmetric formal power series.

9.1. *Chern classes.* Let ξ be a principal $\mathbf{U}(n)$-bundle. Its i-th Chern class is denoted by c_i or $c_i(\xi)$, $(c_i \in H^{2i}(B_\xi, \mathbf{Z}))$, and c or $c(\xi)$ is the sum of the c_i's. It may be defined as follows: let d_j $(1 \leqq j \leqq n)$ be the complex lines spanned by the canonical basis vectors of $\boldsymbol{C}^n$ and let $\boldsymbol{T}$ be the group of diagonal matrices in $\boldsymbol{U}(n)$; the group $\boldsymbol{T}$ is a maximal torus of $\boldsymbol{U}(n)$, its largest subgroup leaving the d_j's invariant. In the universal covering V of $\boldsymbol{T}$, we introduce coordinates x_j such that $x = (x_1, \cdots, x_n)$ operates on d_j by $z \rightarrow z \cdot \exp(2\pi i x_j)$; in other words, x_j is such that, for small positive values of x_j, the product $z \wedge x(z)$ defines the natural orientation of d_j. The restrictions of the x_j to the unit lattice define a basis of $\operatorname{Hom}(H_1(\boldsymbol{T}, \boldsymbol{Z}), \boldsymbol{Z})$ and thus a basis of $H^1(\boldsymbol{T}, \boldsymbol{Z})$, and they are, moreover, permuted by the Weyl group $W(\boldsymbol{U}(n))$ of $\boldsymbol{U}(n)$. Let $y_j = -\tau(x_j)$, where τ is the transgression in $(E_\xi, E_\xi/T, T)$, and let ρ be the projection of $E_\xi/\boldsymbol{T}$ onto B_ξ. Then $y_i \in H^2(E_\xi/T, Z)$ and $c(\xi)$ is defined by

$$\rho^*(c(\xi)) = \prod_1^n (1 + y_i).$$

To legitimize this, we have to know that the right hand side is in the image of ρ^* and that ρ^* is injective. It suffices to prove the first point in the universal bundle, in view of the commutative diagram

$$\begin{tikzcd}
E_\xi \arrow[r] \arrow[d] & E_\xi/\boldsymbol{T} \arrow[r, "\rho"] \arrow[d] & B_\xi \arrow[d, "\sigma"] \\
E_{U(n)} \arrow[r] & E_{U(n)}/\boldsymbol{T} \arrow[r, "\rho'"] & B_{U(n)}
\end{tikzcd}$$

where σ is a characteristic map, but there it follows from [2, § 29] since ρ is by definition $\rho^*(\boldsymbol{T}, \boldsymbol{U}(n))$. As to the second point, $H^*(\boldsymbol{U}(n)/\boldsymbol{T}, \boldsymbol{Z})$ is equal to its characteristic subalgebra [2, Prop. 29. 2]; hence $\boldsymbol{U}(n)/\boldsymbol{T}$ is totally non-homologous to zero in *any* fibre bundle of the type $(E_\xi/\boldsymbol{T}, B_\xi, \boldsymbol{U}(n)/\boldsymbol{T})$, where ξ is a principal $\boldsymbol{U}(n)$-bundle ([2], Cor. to Prop. 18. 3), and this implies, in particular, that ρ^* is injective.

Let us call here a flag or, more precisely, a complex flag an ordered system of n mutually orthogonal 1-dimensional subspaces of $\boldsymbol{C}^n$. Then $\boldsymbol{U}(n)/\boldsymbol{T}$ is the space of flags and $E_\xi/\boldsymbol{T}$ is the total space of the bundle of flags in the complex vector bundle ξ_1 associated to ξ; the bundle η induced from ξ_1 by ρ, with base space $E_\xi/\boldsymbol{T}$, decomposes into a Whitney sum of n $\boldsymbol{C}^1$-vector-bundles with characteristic classes y_i. Thus the present definition of $c(\xi)$ is quite analogous to that of [19, § 4] and, in fact, will be shown in Appendix I to be equivalent to it.

From the properties of ρ^* quoted above, it follows that $\rho^{**}: H^{**}(B_\xi, \boldsymbol{R}) \rightarrow H^{**}(E_\xi/\boldsymbol{T}, \boldsymbol{R})$ is injective and has an image containing the formal power series in the y_i's which are symmetric. Thus we may introduce the *Chern character* ch(ξ) of ξ as an element of $H^{**}(B_\xi, \boldsymbol{R})$ by

$$\rho^*(ch(\xi)) = \exp y_1 + \cdots + \exp y_n = \sum_{j \geqq 0} (j!)^{-1}(y_1{}^j + \cdots + y_n{}^j).$$

Clearly, $ch(\xi)$ and $c(\xi)$, both regarded as elements of $H^{**}(B_\xi, \boldsymbol{R})$, determine each other; $ch(\xi)$ is denoted by $t(\xi)$ in [19].

9.2. *The Stiefel-Whitney classes mod 2.* Let ξ be a principal $\boldsymbol{O}(n)$-bundle; its i-th Stiefel-Whitney class mod 2 is denoted by w_i or $w_i(\xi)$, ($w_i \in H^i(B_\xi, \boldsymbol{Z}_2)$), and the sum of the w_i by w or $w(\xi)$. By naturality, it is enough to define it in the universal bundle. Let $\boldsymbol{Q}$ be the subgroup of diagonal matrices in $\boldsymbol{O}(n)$; we have $H^*(B_{\boldsymbol{Q}(n)}, \boldsymbol{Z}_2) = \boldsymbol{Z}_2[u_1, \cdots, u_n]$, where the u_i's are 1-dimensional classes, which may be assumed to be permuted among themselves by the normalizer of $\boldsymbol{Q}$ in $\boldsymbol{O}(n)$, and $\rho^*(\boldsymbol{Q}, \boldsymbol{O}(n))$ maps $H^*(B_{\boldsymbol{O}(n)}, \boldsymbol{Z}_2)$ isomorphically onto $S(u_1, \cdots, u_n)$. Then w is defined by

$$\rho^*(\boldsymbol{Q}(n), \boldsymbol{O}(n))(w) = \prod_1^n (1 + u_j)$$

(see [3]). This can also be expressed by means of flags. In fact, $\boldsymbol{O}(n)/\boldsymbol{Q}$ is the space of flags (i.e., of ordered systems of n mutually orthogonal lines) in $\boldsymbol{R}^n$ and $(E_\xi/\boldsymbol{Q}, B_\xi, \boldsymbol{O}(n)/\boldsymbol{Q})$ is the bundle of flags in the vector bundle associated to ξ. Let u'_j be the image of u_j under the characteristic map of $(E_\xi, E_\xi/\boldsymbol{Q}, \boldsymbol{Q})$, and let ρ be the projection of $E_\xi/\boldsymbol{Q}$ on B_ξ. Then

$$\rho^*(w(\xi)) = \prod_1^n (1 + u'_j),$$

and this characterizes $w(\xi)$ since ρ^* is injective by [3], Remark on p. 177, and [2], Cor. to Prop. 18.3.

For an $\boldsymbol{SO}(n)$ bundle, the Stiefel-Whitney classes mod 2 are defined as those of the extension to $\boldsymbol{O}(n)$.

9.3. *The Pontrjagin classes.* Let ξ be a principal $\boldsymbol{O}(n)$- or $\boldsymbol{SO}(n)$-bundle. Its i-th Pontrjagin class p_i or $p_i(\xi)$ is the $2i$-th Chern class of the unitary extension of ξ multiplied by $(-1)^i$, and p or $p(\xi)$ is the sum of the p_i's. It may also be characterized in the following way: for $n = 2m$, $2m+1$, let d_j be the 2-dimensional subspaces of $\boldsymbol{R}^n$ spanned by the $(2j-1)$-th and $2j$-th canonical basis vectors, and let $\boldsymbol{T}$ be the maximal subgroup of $\boldsymbol{SO}(n)$ leaving the d_j's invariant; it is a maximal torus. We choose coordinates x_j in its universal covering such that $x = (x_1, \cdots, x_m)$ operates on d_j by means of a rotation of angle $2\pi x_j$; for $n = 2m$, we require that for small positive values of the x_j's, the exterior product $v_j \wedge x(v_j)$ $(v_j \in d_j,\ v_j \neq 0,\ j=1,\cdots,m)$ defines in d_j the same orientation as the $(2j-1)$-th and $2j$-th canonical basis vectors of $\boldsymbol{R}^n$. This determines the x_j's completely. Let us consider the x_j's as a basis of $H^1(\boldsymbol{T},\boldsymbol{Z})$ and put $y_j = -\tau(x_j)$, where τ is the transgression in the universal bundle. It follows from the definition and from the computations made in [2], proof of Prop. 31.4 (see also 9.4), that

$$(1) \qquad \rho_Z^*(\boldsymbol{T},G)(p) = \prod_1^m (1+y_i^2).$$

In § 30, we shall see that

$$(2) \qquad \rho_2^*(\boldsymbol{T},G)(p_i) = w_{2i}^2, \qquad (G=\boldsymbol{SO}(n),\boldsymbol{O}(n)),$$

and that p is completely characterized by (1) and (2). The Pontrjagin classes mod p $(p\neq 2)$, may also be defined by going over to a bundle of flags. In $\boldsymbol{R}^n$ $(n=2m,2m+1)$, we call a 2-flag an ordered system of m mutually orthogonal 2-dimensional oriented subspaces. Then the space of 2-flags in $\boldsymbol{R}^n$ is $\boldsymbol{O}(n)/\boldsymbol{T}$ for n even or $\boldsymbol{O}(n)/\boldsymbol{T}'$ for n odd, where $\boldsymbol{T}'$ is an extension of $\boldsymbol{T}$ by $\boldsymbol{Z}_2$. Let ξ be a principal $\boldsymbol{O}(n)$-bundle and ρ be the projection of $E_\xi/\boldsymbol{T}$ or $E_\xi/\boldsymbol{T}'$ on B_ξ. Then we have

$$\rho^*(p(\xi)) = \prod (1+\tau(x_i)^2),$$

where τ is the transgression in the canonical principal $\boldsymbol{T}$-bundle over $E_\xi/\boldsymbol{T}$ or $E_\xi/\boldsymbol{T}'$ respectively. This is valid over the integers; however ρ^* is injective in general only for the cohomology mod p $(p\neq 2)$, (again by [2], § 29 and Cor. to Prop. 18.3, since $\boldsymbol{SO}(n)$ and $\boldsymbol{O}(n)$ have no p-torsion for $p\neq 2$).

The $(2i+1)$-th Chern class of the complex extension will be denoted $p_{i+\frac{1}{2}}$; it is an element of order 2, equal to the square of the integral $(2i+1)$-th Stiefel-Whitney class (see Appendix II); $\tilde{p}$ or $\tilde{p}(\xi)$ will be the sum of the p_i and $p_{i+\frac{1}{2}}$. We have $\rho_Z^*(\boldsymbol{T},G)(p) = \rho_Z^*(\boldsymbol{T},G)(\tilde{p})$.

9.4. *Remark on the complex extension.* For computational convenience, we shall take as a complex extension of an $\boldsymbol{O}(n)$-bundle the λ-extension, where $\lambda = \delta\circ\gamma$ is the product of the injection $\gamma:\boldsymbol{O}(n)\to\boldsymbol{U}(n)$ and of the inner automorphism $\delta: x\to gxg^{-1}$, the element g being a direct sum of 2×2 matrices

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

and of (1) for odd n; since it is equivalent to the γ-extension, this does not alter the Chern classes. The maximal torus $\boldsymbol{T}$ of $\boldsymbol{O}(n)$, previously described, is then mapped onto the diagonal matrices with coefficients $\exp(\pm 2\pi i x_j)$, and 1 for odd n. We have

$$\lambda^*(x'_{2j+1}) = -\lambda^*(x'_{2j}) = x_j, \qquad (1 \leqq j \leqq [n/2])$$
$$\lambda^*(x'_n) = 0, \quad (n \text{ odd}),$$

where (x_j), (x'_j) are the bases of the first integral cohomology groups of the standard maximal tori of $\boldsymbol{O}(n)$ and $\boldsymbol{U}(n)$ described before.

9.5. *The Euler-Poincaré class.* Let ξ be an oriented vector bundle with $2m$-dimensional fibre, structural group $\boldsymbol{SO}(2m)$, and let η be the associated bundle of unit spheres. The Euler-Poincaré class $W_{2m}(\xi)$ or W_{2m} of ξ is equal to $-\tau(x)$, where x is the generator of $H^{2m-1}(\boldsymbol{S}_{2m-1}, \boldsymbol{Z})$ defined by the positive orientation, and τ is the transgression in η. In the universal case, it is also characterized by the two properties:

(i) W_{2m}, reduced mod 2, is equal to w_{2m},

(ii) $\rho_{\boldsymbol{Z}}^*(\boldsymbol{T}, \boldsymbol{SO}(2m))(W_{2m}) = y_1 \cdot \cdots \cdot y_m.$

For the tangent bundle to a differentiable, compact, connected, oriented manifold, W_{2n} is the fundamental class multiplied by the Euler-Poincaré characteristic.

9.6. *Symplectic Pontrjagin classes.* Let ξ be a $\boldsymbol{Sp}(n)$ bundle and η its extension under the standard inclusion of $\boldsymbol{Sp}(n)$ in $\boldsymbol{U}(2n)$. Its i-th symplectic Pontrjagin class $e_i(\xi)$ or e_i is by definition

$$e_i(\xi) = (-1)^i c_{2i}(\xi),$$

and its total symplectic Pontrjagin class $e(\xi)$ or e is the sum of the e_i's. The computations made in the proof of Prop. 31.3 in [2] show then that the universal symplectic Pontrjagin class satisfies

$$(3) \quad \rho_{\boldsymbol{Z}}^*(T, \boldsymbol{Sp}(n))(e) = \prod_1^n (1 + y_i^2), \quad (T \text{ a maximal torus of } \boldsymbol{Sp}(n)),$$

where the y_i's form a base of $H^2(B_T, \boldsymbol{Z})$ whose elements are permuted, up to sign, by $W(\boldsymbol{Sp}(n))$. Moreover, it follows from ([2], § 9, 29) that $H^*(B_{Sp(n)}, \boldsymbol{Z})$ is the ring of polynomials in the e_i's and that $\rho_{\boldsymbol{Z}}^*(T, \boldsymbol{Sp}(n))$ is injective.

9.7. *The multiplication theorem.* Finally, we recall the Whitney multiplication theorem. Let

$$0 \to \xi' \to \xi \to \xi'' \to 0$$

be an exact sequence of real (resp. complex, resp. quaternionic) vector bundles, with structural group $G=\boldsymbol{O}(n)$ (resp. $\boldsymbol{U}(n)$, resp. $\boldsymbol{Sp}(n)$) for three suitable values of n. Then we have

$$w(\xi)=w(\xi')\cdot w(\xi'') \qquad (G=\boldsymbol{O}(n)), \tag{4}$$

$$\bar{p}(\xi)=\bar{p}(\xi')\cdot\bar{p}(\xi'') \qquad (G=\boldsymbol{O}(n)), \tag{5}$$

$$c(\xi)=c(\xi')\cdot c(\xi'') \qquad (G=\boldsymbol{U}(n)), \tag{6}$$

$$e(\xi)=e(\xi')\cdot e(\xi'') \qquad (G=\boldsymbol{Sp}(n)). \tag{7}$$

(4) and (6) are classical; (5) and (7) follow from (6) and the definitions. We note that, in view of (5), we also have

$$p(\xi)\equiv p(\xi')\cdot p(\xi'') \quad \text{modulo 2-torsion.} \tag{8}$$

These formulae imply, in particular, that w or $\bar{p}$ (resp. c, resp. e) is invariant under an extension relative to the standard inclusion $\boldsymbol{O}(k)\subset\boldsymbol{O}(m)$ (resp. $\boldsymbol{U}(k)\subset\boldsymbol{U}(m)$, resp. $\boldsymbol{Sp}(k)\subset\boldsymbol{Sp}(m)$), $(m\geqq k)$.

10. Representations and characteristic classes.

10.1. *Integral forms as cohomology classes.* Let T be a torus, V its universal covering, Γ the unit lattice, and $\Gamma^*=\mathrm{Hom}(\Gamma,\boldsymbol{Z})$. Thus $\Gamma^*\cong H^1(T,\boldsymbol{Z})$, and, for any commutative group, $\Gamma^*\otimes A\cong H^1(T,A)$. We shall make this identification and, in particular, identify $H^1(T,\boldsymbol{R})$ with V^* and $H^1(T,\boldsymbol{Z})$ with the integral linear forms on V. Also, *the roots* discussed in Chap. I *will be considered in this way as elements of* $H^1(T,\boldsymbol{Z})$ *or* $H^1(T,A)$.

Let ξ be a principal T-bundle. Then τ_ξ maps all of $H^1(T,A)$ in $H^2(B_\xi,A)$. Unless this may lead to a confusion, *we shall denote by the same symbol* $\omega\in\Gamma^*\otimes A$, *the corresponding element in* $H^1(T,A)$, *and* $-\tau_\xi(\omega)\in H^2(B_\xi,A)$.

Let G be a compact connected Lie group and let T be a maximal torus of G. First assume G to be semi-simple and simply connected. Then the transgression in $(G,G/T,T)$ is an isomorphism of $H^1(T,\boldsymbol{Z})$ onto $H^2(G/T,\boldsymbol{Z})$ since G/T is simply connected. Thus the previous conventions identify $H^2(G/T,\boldsymbol{Z})$ and $H^1(T,\boldsymbol{Z})$ with the weights of G (see 3.3). Let G^* be the quotient of G by a finite invariant subgroup and T^* the image of T under the natural map of G onto G^*. Then G/T is homeomorphic to G^*/T^*, as is well known (see e.g. [2], §26); however the transgression in $(G^*,G^*/T^*,T^*)$ will be an isomorphism of $H^1(T^*,\boldsymbol{Z})$ onto the subgroup of $H^2(G/T,\boldsymbol{Z})$ corresponding to the weights which are integral on the unit lattice of G^*. In the general case, let G_1 be the greatest semi-simple subgroup of G (2.9); since maximal tori are maximal abelian subgroups, $T_1 = G_1 \cap T$ is a maximal torus of G_1, and moreover (2.9), G/T may be identified with G_1/T_1. Since a toral subgroup of a torus is always a direct factor, the map $H^1(T, Z) \rightarrow H^1(T_1, Z)$, induced by inclusion, is surjective, and the map: $\mu = (G_1, G_1/T_1, T_1) \rightarrow \nu = (G, G/T, T)$, defined by inclusion, shows then that $\tau_\nu(H^1(T, Z)) = \tau_\mu(H^1(T_1, Z))$.

Let now G' be the quotient of G by a closed subgroup of the center, $\pi: G \rightarrow G'$ the projection, U a connected subgroup of maximal rank in G, $U_1 = G_1 \cap U$, $U' = \pi(U)$. Then rank $U_1 =$ rank G_1, rank $U' =$ rank G', and it follows from 2.9 that $G/U = G_1/U_1$. Also, the argument of [2, § 26] referred to above shows that U is the full inverse image of U' in G, and, consequently, that $G/U = G'/U'$. Therefore, when we deal with coset spaces G/U (rank $G =$ rank U), there is no loss in generality in assuming that G is semi-simple and simply connected.

10.2. *The weights and the character of a homomorphism.* Let G, G' be two compact Lie groups, λ: $G \rightarrow G'$ a homomorphism, T and T' toral subgroups of G and G' such that $\lambda(T) \subset T'$, and (x'_i) a base of $H^1(T, \boldsymbol{Z})$. Then λ induces homomorphisms of $H^1(T', Z)$ and V'^* in $H^1(T, \boldsymbol{Z})$ and V^*, both to be denoted by λ^*. The elements $\omega_i = \lambda^*(x'_i)$, viewed either as elements of $H^1(T, \boldsymbol{Z})$ or as integral linear forms, will be called the (T, T')-weights of λ, or simply the weight of λ when T and T' are maximal.[7] The formal power series

$$ch(\lambda) = \sum \exp \omega_i$$

considered as an element of $H^{**}(B_T, \boldsymbol{R})$ or of $H^{**}(B_\xi, \boldsymbol{R})$, where ξ is a principal T-bundle, will be called the *character* of λ.

Assume now T, T' to be maximal and $G' = \boldsymbol{U}(n)$. Then for $t \in T$, the matrix $\lambda(t)$ is diagonal with the coefficients $\exp(2\pi i \omega_j)$; in other words, the ω_j and the sum of the exponentials of the $2\pi i \omega_j$ are, respectively, the weights and the character of the representation λ in the usual sense.

In the case $G' = \boldsymbol{O}(n)$, i.e., of a real linear representation, we have analogously

$$\lambda(x) = \begin{bmatrix} D(2\pi\omega_1) & & & 0 \\ & \cdot & & \\ & & \cdot & \\ 0 & & & \cdot \\ & & & D(2\pi\omega_m) \end{bmatrix} \qquad \lambda(x) = \begin{bmatrix} D(2\pi\omega_1) & & & & 0 \\ & \cdot & & & \\ & & \cdot & & \\ 0 & & & \cdot & \\ & & & D(2\pi\omega_m) & \\ & & & & 1 \end{bmatrix}$$

---

[7] More precisely, with respect to the basis (x'_i), which is always supposed to be chosen as in § 9 when G' is a classical group.

for $n = 2m$ and $n = 2m + 1$ respectively, where $D(\alpha)$ is a 2-dimensional rotation of angle α; the weights of λ, considered as a representation in $\boldsymbol{U}(n)$, are then the forms $\pm\,\omega_j$, together with the zero form for odd n.

10.3. THEOREM. *Let G, G' be two compact Lie groups, $\lambda\colon G \to G'$ a homomorphism, T, T' maximal tori of G and G' such that $\lambda(T) \subset T'$, and (ω_j) the weights of λ. Let ξ be a principal G-bundle, η its λ-extension, ρ the projection of E_ξ/T onto B_ξ. Then*

(a) *If $G' = \boldsymbol{U}(m)$, then*

$$\rho^*(c(\eta)) = \prod(1 + \omega_j)\,;\ \rho^{**}(ch(\eta)) = ch\,\lambda.$$

(b) *If $G' = \boldsymbol{SO}(m)$ or $\boldsymbol{O}(m)$, the Pontrjagin class $p(\eta)$ satisfies*

$$\rho^*(p(\eta)) = \rho^*(\tilde{p}(\eta)) = \prod(1 + (\omega_j)^2).$$

(c) *If $G' = \boldsymbol{SO}(2m)$, the Euler-Poincaré class $W_{2m}(\eta)$ satisfies*

$$\rho^*(W_{2m}(\eta)) = \prod \omega_j.$$

(a) We have a commutative diagram

$$\begin{tikzcd} E_\xi \arrow[r] \arrow[d, "\phi"'] & E_\xi/T \arrow[r, "\rho"] \arrow[d, "\phi_1"] & B_\xi \arrow[d] \\ E_\eta \arrow[r] & E_\eta/T' \arrow[r, "\rho'"] & B_\xi, \end{tikzcd} \tag{1}$$

where ϕ is a λ-map. By (9.1), putting c' for $c(\eta)$, we have

$$\rho'^*(c') = \prod(1 - \tau'(x'_i)),$$

where τ' is the transgression in $(E_\eta, E_\eta/T', T')$; and therefore

$$\rho^*(c') = \phi_1^* \cdot \rho'^*(c') = \prod(1 - \phi_1^*\tau'(x_j')).$$

Since ϕ commutes with transgression, this gives

$$\rho^*(c') = \prod(1 - \tau\lambda^*(x'_j))$$

and our assertion follows from the definition of the weights and the notation convention of (10.1). The proofs for (b) and (c) are similar.

10.4. COROLLARY. *Let $G = \boldsymbol{U}(n)$, $G' = \boldsymbol{U}(m)$, $\boldsymbol{T}$ the standard maximal torus of G, $\omega_j = \sum_i a_{ij}x_i$ the weights of λ expressed in terms of the canonical basis of $H^1(\boldsymbol{T}, \boldsymbol{Z})$, $(i = 1, \cdots, n; j = 1, \cdots, m)$. Then*

$$c(\eta) = \prod(1 + \sum_i a_{ij}y_i)$$

where the y_i's are formally defined by $c(\xi) = \prod(1+y_i)$. *The class* $c(\eta)$ *is a polynomial with integral coefficients in the classes* $c_i(\xi)$.

By (9.1), we have $\rho^*(c(\xi)) = \prod(1-\tau(x_i))$, and our first assertion follows from 10.3 and the fact that ρ^* is injective when G is the unitary group. Moreover, the Weyl group $W(\boldsymbol{U}(n))$ operates in a natural way on the fibration $(E_\xi/\boldsymbol{T}, B_\xi, \boldsymbol{U}(n)/\boldsymbol{T}, \rho)$ and induces the identity on B_ξ (see [2], § 27). Therefore the image of ρ^*, and in particular, $\rho^* c(\eta)$, is made up of invariants of $W(\boldsymbol{U}(n))$; since the latter is the group of permutations of the x_i, or equivalently, of the $\tau(x_i)$, it follows that $c(\eta)$ is a symmetric function in the y_i's, whence our second assertion.

10.5. Corollary. *Let* $G = \boldsymbol{O}(n)$ *or* $\boldsymbol{SO}(n)$, G' *be* $\boldsymbol{O}(m)$ *or* $\boldsymbol{SO}(m)$. *Then* $p(\eta)$ *reduced* mod p $(p \neq 2)$, *is a polynomial in the* $p_i(\xi)$, *and if* $G = \boldsymbol{SO}(2m)$, *in* $W_{2m}(\xi)$. *If* λ *can be extended to a homomorphism of* $\boldsymbol{U}(n)$ *into* $\boldsymbol{U}(m)$, *then* $\tilde{p}(\eta)$ *is a polynomial in the classes* $p_i(\xi)$, $p_{i+\frac{1}{2}}(\xi)$, *and, in particular,* $p(\eta)$ *reduced* mod p $(p \neq 2)$, *is a polynomial in the classes* $p_i(\xi)$.

The first assertion is proved in the same way as 10.4, using 9.3, 9.5 and the properties of the invariants of $W(G)$ recalled in 30.2. The second one follows from 10.4 by considering the Pontrjagin classes as the Chern classes of the complex extension.

10.6. *Examples.* (a) Let ξ be a complex vector bundle, ξ^* the dual bundle. Then, if $c(\xi) = \prod(1+x_i)$, we have $c(\xi^*) = \prod(1-x_i)$. In fact, the principal bundle θ associated to ξ^* is the λ-extension of the principal bundle of ξ, where λ is the contragredient representation, whose weights are obviously the forms $-x_i$.

(b) Let $G = \boldsymbol{U}(n)$, j be a positive integer $\leqq n$, and λ the natural representation of $\boldsymbol{U}(n)$ in the j-th exterior power $\wedge^j \boldsymbol{C}^n$ of $\boldsymbol{C}^n$. Let (e_i) be the canonical base of $\boldsymbol{C}^n$. Then the products

$$e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_j} \qquad (1 \leqq i_1 < \cdots < i_j \leqq n)$$

form a base of $\wedge^j \boldsymbol{C}^n$, and we have

$$\lambda(x)(e_{i_1} \wedge \cdots \wedge e_{i_j}) = \exp[2\pi i(x_{i_1} + \cdots + x_{i_j})](e_{i_1} \wedge \cdots \wedge e_{i_j});$$

i.e., the weights of λ are the sums

$$x_{i_1} + \cdots + x_{i_j}, \qquad (1 \leqq i_1 < \cdots < i_j \leqq n).$$

Here η is the principal bundle associated to the bundle of contravariant p-

vectors in the complex vector bundle associated to ξ. This bundle has, therefore, as Chern class

$$c' = \prod_{1 \leqq i_1 < \cdots < i_j \leqq n} (1 + x_{i_1} + \cdots + x_{i_j}).$$

(c) In the same way, the Chern class of the bundle of contravariant symmetric tensors of degree j will be

$$\prod_{1 \leqq i_1 \leqq \cdots \leqq i_j \leqq n} (1 + x_{i_1} + \cdots + x_{i_j}).$$

(d) Let ξ_i $(i = 1, 2)$, be two complex vector bundles over B and let

$$c_{(i)} = \prod_{j=1}^{n_i} (1 + x_j^{(i)})$$

be formal decompositions of their Chern polynomials. Then

$$c(\xi_1 \otimes \xi_2) = \prod_{i=1}^{n_1} \prod_{j=1}^{n_2} (1 + x_i^{(1)} + x_j^{(2)}).$$

To see this, we take as ξ the principal bundle with group $\boldsymbol{U}(n_1) \times \boldsymbol{U}(n_2)$ associated to the sum $\xi_1 \oplus \xi_2$, whose Chern class is $c_{(1)} \cdot c_{(2)}$ by the multiplication theorem (9.7), and as λ the representation of $\boldsymbol{U}(n_1) \times \boldsymbol{U}(n_2)$ in $\boldsymbol{U}(n_1 \cdot n_2)$ defined by $(g_1, g_2) \to g_1 \otimes g_2$, considered as an automorphism of $\boldsymbol{C}^{n_1} \otimes \boldsymbol{C}^{n_2}$. The products $e_i \otimes f_j$, where (e_i) and (f_j) are the canonical bases of $\boldsymbol{C}^{n_1}$ and $\boldsymbol{C}^{n_2}$, form a base of $\boldsymbol{C}^{n_1} \otimes \boldsymbol{C}^{n_2}$; hence the weights of λ are the forms $x_i^{(1)} + x_j^{(2)}$, and our contention follows from (10.3) and from the fact that the λ-extension of ξ is the principal bundle of $\xi_1 \otimes \xi_2$.

(e) To compute the Pontrjagin classes of real vector bundles, it is often more convenient to look at the Chern classes of the complex extensions; as an illustration, we take the case where $G = \boldsymbol{SO}(2n)$ and λ is the representation in $\bigwedge^2 \boldsymbol{R}^{2n}$. Let μ, ν denote the complex extensions of ξ, η (as defined in 9.4), let $\mathbf{T}$, $\mathbf{T}'$ be the standard maximal tori of $\boldsymbol{SO}(2n)$, $\boldsymbol{U}(2n)$, and let (x_i), (x_i') be the canonical bases of $H^1(\boldsymbol{T}, Z)$ and $H^1(\boldsymbol{T}', Z)$. We have a commutative diagram

$$\begin{tikzcd}
E_\xi \arrow[r] \arrow[d, "\phi"'] & E_\xi/\boldsymbol{T} \arrow[r, "\rho"] \arrow[d, "\phi_1"'] & B_\xi \arrow[d, "\mathrm{Id}"] \\
E_\mu \arrow[r] & E_\mu/\boldsymbol{T}' \arrow[r, "\sigma"] & B_\xi,
\end{tikzcd}$$

and it follows from (9.4), (10.3) that

$$x_i = \lambda^*(x'_{2i-1}) = -\lambda^*(x'_{2i}), \qquad (1 \leqq i \leqq n),$$

$$\rho^*(p(\xi)) = \prod_1^n (1 + x_i^2),$$

$$\sigma^*(c(\mu)) = \prod_1^{2n} (1 + x'_j).$$

Now, ν is clearly the extension of μ corresponding to the "complexification of λ," i. e., to the natural representation of $\boldsymbol{U}(2n)$ in $\wedge^2 \boldsymbol{C}^{2n}$; therefore, by example (b),

$$\sigma^*(c(\nu)) = \prod_{1 \leqq i < j \leqq 2n} (1 + x'_i + x'_j).$$

This gives

$$\phi^*{}_1 \cdot \sigma^*(c(\nu)) = \prod_{1 \leqq i < j \leqq n} (1 - (x_i + x_j)^2) \cdot (1 - (x_i - x_j)^2),$$

$$\rho^*(c(\nu)) = \prod_{1 \leqq i < j \leqq n} [(1 - x_i^2 - x_j^2)^2 - 4 \cdot x_i^2 \cdot x_j^2],$$

and finally

$$\rho^*(\tilde{p}(\eta)) = \rho^*(p(\eta)) = \prod_{1 \leqq i < j \leqq n} [(1 + x_i^2 + x_j^2)^2 - 4 \cdot x_i^2 \cdot x_j^2].$$

(f) It may be shown in the same way that if ξ_1, ξ_2 are two real vector bundles over the same base space B with Pontrjagin classes reduced mod p $(p \neq 2)$, equal to

$$p(\xi_1) = \prod_1^m (1 + x_i^2), \qquad p(\xi_2) = \prod_1^n (1 + y_j^2),$$

then

$$p(\xi_1 \otimes \xi_2) = \prod_{i=1}^m \prod_{j=1}^n (1 + (x_i + x_j)^2) \cdot (1 + (x_i - x_j)^2).$$

10. 7. Theorem. *Let G be a compact connected Lie group, U a closed subgroup of G, S a maximal torus of U, and $(\pm b_j)$ $(1 \leqq j \leqq k)$, the roots of G with respect to S which are complementary to those of U. Let ξ be a principal G-bundle, ρ the projection of E_ξ/S onto E_ξ/U, and η the bundle along the fibres (7.4) of $(E_\xi/U, B_\xi, G/U)$. Then $\rho^*(\tilde{p}(\eta)) = \prod (1 + b_j^2)$; if, moreover, U is connected and $\dim G/U = m$ is even, then $\rho^*(W_m(\eta)) = \pm \prod b_j$.*

By (7.5), η is the ι-extension of $(E_\xi, E_\xi/U, U)$, where ι is the isotropy representation; according to the definitions in (1.3) and (10.1), the b_j's are the weights of ι (up to a certain number of zero forms, but this does not alter our formulas), and (10.7) follows then from (10.3). The sign for the Euler-Poincaré class will be determined by the conventions made in 9.5, once the bundle along the fibres has been oriented.

10.8. We keep the previous notations. Let J be an invariant almost complex structure on G/U and η' be the complex vector bundle structure of η constructed by means of J (see 7.4). J is defined by a complex structure on the tangent space $(G/U)_0$, invariant under U; this complex structure gives rise to a linear representation ι_c of U in $\boldsymbol{C}^{m/2}$ $(m = \dim G/U)$, which goes over to ι by taking real and imaginary parts. The weights of ι_c are some of the forms $\pm b_j$, and (10.3) also implies:

THEOREM. *We keep the notations of* 10.7; *assume, moreover, that G/U has an invariant almost complex structure J, and denote by η' the complex vector bundle structure of η associated to J. Then* $\rho^*(c(\eta')) = \prod_{j \in J} (1 + \epsilon_j b_j)$, $(\epsilon_j = \pm 1)$, *where $\epsilon_j b_j$ runs through the weights of the complex isotropy representation ι_c defining J.*

The weights of ι_c will be discussed in detail for the case where $\operatorname{rank} G = \operatorname{rank} U$ in Chapter IV.

10.9. In order to study the tangent bundle to G/U it is usually convenient to consider the bundle $\hat{\theta}$ along the fibres of $(B_U, B_G, G/U, \rho(U, G)) = \theta$ and restrict to a fibre of θ, since this allows one to make use of known results about classifying spaces. We consider here, in particular, the case where $U = T$ is a maximal torus and show the

PROPOSITION. *Let T be a maximal torus of G. Then the total Pontrjagin class $\bar{p}(\mu)$ of the tangent bundle μ to G/T is* 1.

Let $\theta = (B_T, B_G, G/T)$ and let i be the inclusion map of a fibre. $H^*(G/T, \boldsymbol{Z})$ is torsion free ([5], or R. Bott, *Bull. Soc. Math. France* 84, (1956) 251-281), and therefore the subgroup S of invariants of $W(G)$ in $H^*(G/T, \boldsymbol{Z})$ is a free abelian group; since by a lemma of Leray (see [2], Lemma 27.1), $H^*(G/T, \boldsymbol{R})$ is the space of the regular representation of $W(G)$, it follows that $S = H^0(G/T, \boldsymbol{Z})$ and that the kernel of i^* contains the subgroup I_G^+ of invariants of $W(G)$ in $H^*(B_T, \boldsymbol{Z})$ having strictly positive degrees.

By (10.7) we have

$$\bar{p}(\hat{\theta}) = \prod (1 + b_j^2),$$

where the $\pm b_j$'s are the roots of G. Since $W(G)$ permutes the b_j^2, it leaves $\bar{p}(\hat{\theta})$ invariant, whence

$$\bar{p}(\mu) = i^*(\bar{p}(\hat{\theta})) = 1.$$

11. Representations and Stiefel-Whitney classes. In this section, Q, Q' denote commutative groups of type $(2,2,\cdots,2)$. The following discussion applies to any arbitrary compact Lie group, but has an interest only for groups in which maximal commutative subgroups of type $(2,\cdots,2)$ are conjugate and play in cohomology mod 2 the role of maximal tori in real cohomology. We therefore assume tacitly that G, G' are products of copies of $\boldsymbol{O}(n)$, $\boldsymbol{SO}(n)$, $\boldsymbol{U}(n)$, $\boldsymbol{SU}(n)$, $\boldsymbol{Sp}(n)$, $\boldsymbol{G}_2$ (see [3]).

11.1. *Characters of Q as cohomology classes.* Q being discrete, $H^*(B_Q,A)$ is the cohomology ring of Q in the sense of Hopf-Eilenberg-MacLane, and, in particular, $H^1(B_Q,A)=\mathrm{Hom}(Q,A)$. Thus $x\in\mathrm{Hom}(Q,A)$ may be considered as a 1-dimensional cohomology element in B_Q or, via the characteristic map, in the base space of any principal bundle (E,B,Q), which will be usually denoted by the same symbol $(x\in H^1(B,A))$ in particular, the 2-roots introduced in § 5 will be considered as elements of $H^1(B,\boldsymbol{Z}_2)$. We note that if $\lambda\colon Q\to Q'$ is a homomorphism, then

$$\rho(\lambda)^*\colon H^1(B_{Q'},A)\to H^1(B_Q,A) \text{ and } \lambda'\colon \mathrm{Hom}(Q',A)\to\mathrm{Hom}(Q,A)$$

are carried into one another by the previous identification.

11.2. *The 2-weights of a homomorphism.* Let $\lambda\colon G\to G'$ be a homomorphism, Q, Q' maximal and such that $\lambda(Q)\subset Q'$, and (x_i), (x'_i) bases of $\mathrm{Hom}(Q,\boldsymbol{Z}_2)$ and $\mathrm{Hom}(Q',\boldsymbol{Z}_2)$, considered as Z_2-modules. Then λ^*: $\mathrm{Hom}\,(Q',\boldsymbol{Z}_2)\to\mathrm{Hom}\,(Q,\boldsymbol{Z}_2)$ is characterized by elements $\omega_j=\lambda^*(x'_j)=\sum a_{ij}x_i$, to be called the *2-weights of* λ. Here, also, we assume, in case of an orthogonal group, the basis to be chosen as in (9.2).

11.3. THEOREM. *Let G be a compact Lie group, Q a maximal commutative subgroup of type $(2,\cdots,2)$, $\lambda\colon G\to\boldsymbol{O}(n)$ a homomorphism, (ω_j) its 2-weights, ξ a principal bundle, ξ' its λ-extension, and ρ the projection of E/Q onto B. Then $\rho^*(w(\xi'))=\prod(1+\omega_j)$.*

The proof is the same as for (10.3), except that instead of (1) § 10, we use the commutativity of the diagram

$$\begin{tikzcd} E_\xi/Q \arrow[r, "\phi'"] \arrow[d, "\sigma"] & E_\xi/Q' \arrow[d, "\sigma'"] \\ B_Q \arrow[r] & B_{Q'}, \end{tikzcd}$$

where σ and σ' are characteristic maps, and the end remark of (11.1); therefore, we shall not reproduce it here.

Remark. For the groups mentioned at the beginning of § 11, ρ^* is injective [3].

11.4. COROLLARY. *Assume, moreover, that* $G = \boldsymbol{O}(n)$. *Then* $w(\xi') = \prod (1 + \sum a_{ij} x_i)$, *where the* x_i *are the formal roots of* $w(\xi)$. *In particular,* $w(\xi')$ *is a polynomial in the classes* $w_i(\xi)$.

Same proof as for (10.4), except that instead of using the Weyl group, we take the quotient by Q of its normalizer in $\boldsymbol{O}(n)$; its inner automorphisms also induce the group of permutations of the x_i's.

Examples. Computations paralleling those of 10.6, (b), (c), (d) will lead to the same formulas for the Stiefel-Whitney classes of bundles of p-vectors, symmetric tensors, and for tensor products, the x_i and y_j standing now for 1-dimensional classes mod 2. Details are left to the reader.

11.5. THEOREM. *Let* G *be a compact Lie group,* U *a closed subgroup, and* Q *a maximal commutative subgroup of type* $(2, \cdots, 2)$ *of* U. *Let* ξ *be a principal* G-*bundle,* ρ *the projection of* E_ξ/Q *on* E_ξ/U, *and* η' *the bundle along the fibres* G/U. *Then*

$$\rho^*(w(\eta')) = \prod (1 + a_i),$$

where the a_i's *are the 2-roots of* G *with respect to* Q, *complementary to those of* U.

The a_i's are the 2-weights of the isotropy representation; hence (11.5) follows from (7.5) and (11.3).

Applications will be given in Chapter V.

Chapter IV. Roots and Invariant Almost Complex Structures.

In this chapter, G is a compact, connected, semi-simple, Lie group, l its rank, U a proper closed connected subgroup of the same rank, and T a maximal torus of U. If ψ is a set of roots, we put $-\psi = \{-a, a \in \psi\}$.

12. Integrability of invariant almost complex structures. We recall here some known facts in a form convenient for the sequel.

12.1. Let V be a real $2n$-dimensional vector space, endowed with a complex structure defined by a linear transformation J, and let V^c be its complexification. Then

$$V^c = T^+ + T^-, \qquad T^- = \overline{T^+}, \qquad T^+ \cap T^- = (0),$$

where T^+ (resp. T^-) is the eigenspace of the extension J^c of J to V^c corresponding to the eigenvalue $+i$ (resp. $-i$) and where the bar denotes complex conjugation with respect to V. Conversely, given such a decomposition of V^c, we define J^c by $J^c(x) = i \cdot x$ $(x \in T^+)$, $J^c(x) = -ix$, $(x \in T^-)$; then J^c leaves V invariant and induces there a complex structure such that $x \to x + \bar{x}$ is a complex isomorphism $(x \in T^+)$. In particular, given a linear transformation A without real eigenvalues, we define T^+ (resp. T^-) as the sum of the eigenspaces of its semi-simple part corresponding to eigenvalues with positive (resp. negative) imaginary parts, and thus attach to A a complex structure on V.

12.2. The roots of G with respect to T define linear forms on the Lie algebra $\mathfrak{t}$ of T, and it follows from (1.3) and standard facts about the adjoint representation that

$$\operatorname{ad} x\,|_{\mathfrak{a}_i} = \begin{pmatrix} 0 & -2\pi a_i(x) \\ 2\pi a_i(x) & 0 \end{pmatrix}, \quad (x \in \mathfrak{t}),$$

$\operatorname{ad} x$ being defined by $(\operatorname{ad} x)(y) = [x, y]$, $(x, y \in \mathfrak{g})$.

We have then, superscripts denoting complexification, that

$$\mathfrak{g}^c = \mathfrak{t}^c + \mathfrak{a}_1{}^c + \cdots + \mathfrak{a}_m{}^c, \qquad \mathfrak{a}_i{}^c = \mathfrak{d}_{a_i} + \mathfrak{d}_{-a_i},$$

$$[x, e_{\pm a_j}] = \pm 2\pi i a_j(x) e_{\pm a_j}, \qquad (e_{\pm a_j} \in \mathfrak{d}_{\pm a_j});$$

since any two roots are different from each other, the 1-dimensional eigenspaces $\mathfrak{d}_{\pm a_j}$ are well determined by $\mathfrak{t}$. We recall that if α, β are two roots, we have

$$\begin{aligned} &[\mathfrak{d}_\alpha, \mathfrak{d}_\beta] = 0 && \text{if } \alpha + \beta \text{ is not a root and not zero,} \\ (1) \qquad &[\mathfrak{d}_\alpha, \mathfrak{d}_\beta] = \mathfrak{d}_{\alpha+\beta} && \text{if } \alpha + \beta \text{ is a root,} \\ &[\mathfrak{d}_\alpha, \mathfrak{d}_{-\alpha}] \subset \mathfrak{t}^c, \ [\mathfrak{d}_\alpha, \mathfrak{d}_{-\alpha}] \neq 0. \end{aligned}$$

12.3. Assume now that G/U has been endowed with an invariant almost complex structure and let $\pm b_j$ $(1 \leqq j \leqq k)$ be the complementary roots. The almost complex structure is characterized by a linear transformation J, $(J^2 = -\mathrm{Id})$, of $(G/U)_0$ which commutes with the linear isotropy group (1.1). Since $b_i \neq b_j$ for $i \neq j$, J must also leave the subspaces $\mathfrak{b}_i$ invariant and it induces complex structures on them which characterize it completely. Now on each $\mathfrak{b}_j$ there are two complex structures commuting with the isotropy representation of T in $\mathfrak{b}_j$, differing by the orientation they induce; to each b_j we attach a sign ϵ_j, equal to $+1$ (resp. -1), according to whether the ordered pairs $(e, \operatorname{Ad} t(e))$ and $(e, J(e))$ define the same orientation or not

($e \in \mathfrak{b}_j, e \neq 0, t \in T$ such that $0 < b_j(t) < \frac{1}{2}$). The $\epsilon_j b_j$ will be called *the roots of the almost complex structure,* which they describe completely.

We extend J to a linear transformation $\tilde{J}$ of $\mathfrak{g}$ by putting it equal to zero on $\mathfrak{u}$, and to a linear transformation $\bar{J}^c$ of $\mathfrak{g}^c$; it is readily seen that

$$\bar{J}^c(e_{\epsilon_j b_j}) = i \cdot e_{\epsilon_j b_j}; \; \bar{J}^c(e_{-\epsilon_j b_j}) = -i \cdot e_{\epsilon_j b_j} (e_{\pm b_j} \in \mathfrak{b}_{\pm b_j}).$$

The space T^+ of (12.1) may be identified with the space spanned by the $v_{\epsilon_j b_j}$ which, by the foregoing, is invariant under $\mathrm{Ad}_G U$. Since $x \rightarrow x + \bar{x}$ is a complex isomorphism of T^+ onto $(G/U)_0$, the previous identification carries the restriction of $\mathrm{Ad}_G U$ onto the complex isotropy representation ι_c defined in § 10, and, therefore, *the $\epsilon_j b_j$ are the weights of ι_c.*

The almost complex structure is integrable, i. e. (since we are in the real analytic case), derives from an automatically invariant complex analytic structure, if and only if

$$\mathfrak{n} = \mathfrak{u}^c + \mathfrak{b}_{\epsilon_1 b_1} + \cdot \cdot \cdot + \mathfrak{b}_{\epsilon_k b_k}$$

is a Lie algebra [14, § 20]. In view of the properties of the bracket recalled above, this proves the first assertion of:

12. 4. Lemma. *Let $\mathcal{J}$ be an invariant almost complex structure on G/U, ψ the system of its roots, and Σ the system of roots of U. Then $\mathcal{J}$ is integrable if and only if $\Sigma \cup \psi$ is closed in the sense of § 4. In this case, ψ is closed and contained in a system of positive roots.*

As to the second assertion, we remark that by 4. 10, we have $\Sigma = \theta \cup -\theta$, where $\theta \cup \psi$ is a system of positive roots for some ordering. Since $\Sigma \cup \psi$ and $\theta \cup \psi$ are closed and since $\psi \cap -\psi = \phi$, it follows immediately that ψ is closed.

More precise statements about ψ will be given in 13. 7.

13. Applications.

13. 1. The following known facts will be used in this section. A compact connected Lie group K is semi-simple if and only if $H^1(K, \boldsymbol{R}) = 0$, and then $H^2(K, \boldsymbol{R}) = 0$ (see, e. g., Chevalley-Eilenberg, Trans. Amer. Math. Soc., 63 (1948), 85-124). A simple spectral sequence argument then shows that, if K is compact and semi-simple and L is a closed connected subgroup, the transgression is an isomorphism of $H^1(L, \boldsymbol{R})$ onto $H^2(K/L, \boldsymbol{R})$, and, in particular, that $H^2(K/L, \boldsymbol{R}) = 0$ if and only if L is semi-simple, too.

13. 2. *Coset spaces with second Betti number zero.* As a first application

of §§ 4 and 10, we prove anew a theorem of H. C. Wang [31, Theorem C] to the effect that *a coset space G/U with* $\operatorname{rank} G = \operatorname{rank} U$ *and second Betti number zero is not homogeneous complex.*

Assume that G/U has an invariant almost complex structure with roots $(\epsilon_j b_j)$, $(1 \leqq j \leqq k)$; let c_1 be its first Chern class and ρ be the projection of G/T onto G/U. By (10.8) and (12.3),

$$\rho^*(c_1) = -\tau(\epsilon_1 b_1 + \cdots + \epsilon_k b_k)$$

(τ transgression in $(G, G/T, T)$). Since $H^2(G/U, \boldsymbol{R}) = 0$, c_1 must be a fortiori zero as a real cohomology class, and hence, by (13.1), $\sum \epsilon_j b_j = 0$. But then, by § 4, the system $(\epsilon_j b_j)$ does not satisfy the condition of 12.4, and thus the almost complex structure is not integrable.

13.3. *Examples of* (13.2). Now let G be simple and U be a maximal connected subgroup of maximal rank. A complete list of such inclusions is given in [7]; to discuss it, we assume, moreover, the center of G to be reduced to the identity, which is no loss in generality. These inclusions may then be divided into three classes:

(a) U is the connected centralizer of an element of order 2, which generates its center.

(b) U is the centralizer of a one dimensional torus S, and S is the identity component of the center of U.

(c) U is the connected centralizer of an element z of order 3 or 5, which generates its center.

The coset spaces G/U corresponding to the classes (a), (b) are irreducible Riemannian and hermitian symmetric spaces respectively. In the class (c) we find seven spaces, namely $\boldsymbol{G}_2/\boldsymbol{A}_2 = \boldsymbol{S}_6$, $\boldsymbol{F}_4/\boldsymbol{A}_2 \times \boldsymbol{A}_2$, $\boldsymbol{E}_6/\boldsymbol{A}_2 \times \boldsymbol{A}_2 \times \boldsymbol{A}_2$, $\boldsymbol{E}_7/\boldsymbol{A}_2 \times \boldsymbol{A}_5$, $\boldsymbol{E}_8/\boldsymbol{A}_8$, $\boldsymbol{E}_8/\boldsymbol{A}_2 \times \boldsymbol{E}_6$ for z of order 3 and $\boldsymbol{E}_8/\boldsymbol{A}_4 \times \boldsymbol{A}_4$ for z of order 5.

U being the connected centralizer of z, its algebra $\mathfrak{u}$ is the set of fixed points under $\operatorname{Ad} z$; consequently, $\operatorname{Ad} z$ has no real eigenvalues on the complementary subspaces $\mathfrak{b}_j$, and we may attach to it a complex structure on $(G/U)_0$, as recalled in (12.1), which will be invariant under U, since the latter commutes with $\operatorname{Ad} z$, and defines, consequently, an invariant almost complex structure on G/U. Here since U has a discrete center, it is semi-simple, and $H^2(G/U, R) = 0$ (see 13.1). Therefore, by (13.2), we have the

PROPOSITION. *The seven coset spaces of the class* (c) *above are homogeneous almost complex but not homogeneous complex.*

This generalizes a known result for S_6 (Ehresmann Libermann, *C. R. Acad. Sci. Paris* 232 (1951), 1281 [14, § 10]).

13.4. PROPOSITION. *Let G/U be homogeneous almost complex, and let $\iota = \iota_1 + \cdots + \iota_s$ be a decomposition of the isotropy representation into real irreducible representations; then the ι_i are unique, each one has the complex numbers as commuting field, and G/U admits exactly 2^s invariant almost complex structures.*

Let $(G/U)_0 = W_1 + \cdots + W_s$ be a direct sum decomposition of $(G/U)_0$ such that the restriction of ι to W_i is ι_i. Since these subspaces are invariant under T, they are direct sums of subspaces $\mathfrak{b}_j$, and the corresponding roots $\pm b_j$ are the weights of ι_i; since any two roots are different, the complex irreducible components of the ι_i will be pairwise inequivalent, from which follows the uniqueness of the ι_i and of the W_i. Also, a straightforward application of Schur's lemma shows that any linear transformation commuting with ι leaves the W_i's invariant. Since, by assumption, there is at least one transformation without real eigenvalues commuting with ι, we see that the commuting field of ι_i is either the field of complex numbers $\boldsymbol{C}$ or of quaternionic numbers $\boldsymbol{K}$; in any case ι_i is not complex irreducible and its extension to $W_i \otimes \boldsymbol{C}$ decomposes into $\gamma_i + \bar{\gamma}_i$, where γ_i is complex irreducible and $\bar{\gamma}_i$ is the complex conjugate representation of γ_i; the weights of $\bar{\gamma}_i$ are opposite in sign to the weights of γ_i. Since the roots of G are pairwise distinct (§ 2), γ_i is not equivalent to $\bar{\gamma}_i$, and it follows from Schur's lemma again that the commuting field of ι_i is the field of complex numbers. Thus we have on each W_i exactly 2 invariant complex structures, from which our contention follows.

Remark. Let σ be an automorphism of G leaving T and U invariant, $d\sigma$ the induced automorphism of $\mathfrak{g}$; let ψ be the root system of an invariant almost complex structure $\mathcal{J}$ on G/U, and ψ' the transform of ψ under $d\sigma$. From the formula (1) in § 1, it follows readily that the homeomorphism σ' of G/U defined by σ carries $\mathcal{J}$ onto the invariant almost complex structure with roots ψ'. If, in particular, $\sigma(x) = g \times g^{-1}$ with $g \in N_T \cap U$, then σ' reduces to the left translation defined by g and leaves $\mathcal{J}$ invariant; hence the element of $W(U)$ represented by g must leave ψ invariant.

13.5. *Centralizers of tori.* The following proposition is due to H. C. Wang [31]:

PROPOSITION. *G/U (with* $\operatorname{rank} U = \operatorname{rank} G$; *$U$ connected) is homogeneous complex if and only if U is the centralizer of a torus in G.*

Proof. Let U be the centralizer of a torus S, which we assume, as we may, to be in T, and let $s \in S$ generate an everywhere dense subgroup of S. Then U is the centralizer of s, $\mathfrak{u}$ the space of vectors fixed under $\operatorname{Ad} s$, and we have $b_j(s) \not\equiv 0\,(1)$ if and only if b_j is complementary. Let $\epsilon_j = \operatorname{sgn}\,(b_j(s))$ $(1 \leqq j \leqq k)$; since s centralizes U, the $\epsilon_j b_j$ are the roots of an invariant almost complex structure; moreover, being characterized by $\epsilon_j b_j(s) > 0$, these roots satisfy the criterion of 12.4, and the structure is integrable.

Assume now, conversely, that G/U has been endowed with a homogeneous complex structure and let $(\epsilon_j b_j)$ $(1 \leqq j \leqq k)$, be its roots. By (2.9), the group is locally isomorphic to the direct product of its largest semi-simple subgroup U' and of a torus S; moreover, by 13.1 and 13.2, $S \neq \{e\}$. Now let W be the centralizer of S. We have $W = S_1 \cdot W'$, where S_1 is a torus containing S and W' a semi-simple subgroup containing U' and $W' \cap S_1$ is finite. The equalities

$$\operatorname{rank} G = \operatorname{rank} U' + \dim S = \operatorname{rank} W' + \dim S_1$$

show then that $S = S_1$, that $\operatorname{rank} W' = \operatorname{rank} U'$, and that W/U is to be identified with W'/U'; since W' and U' are semi-simple, we have $H^2(W'/U', \mathbf{R}) = 0$ and W/U is not homogenous complex (13.1, 13.2).

Let $J \subset [1, k]$ be such that the $\pm\, b_j$'s, with $j \in J$, are the complementary roots of U in W. The roots $(\epsilon_j b_j)$ $(j \in J)$, define a complex structure on $(W/U)_0$ which is invariant under the linear isotropy representation ι' of U in $(W/U)_0$ since ι' is nothing but the restriction to an invariant subspace of the isotropy representation of U in $(G/U)_0$; moveover, since the system $(\epsilon_j b_j)$ $(1 \leqq j \leqq k)$, satisfies the condition of 12.4, so does $(\epsilon_j b_j)$ $(j \in J)$. Therefore, if $W \neq U$, then we get on W/U an invariant integrable almost complex structure, in contradiction to what has already been proved. Thus $U = W$ and U is the centralizer of the torus S.

13.6. For the sake of completeness, we recall the proof of the following well-known lemma.

LEMMA. *Let U be the centralizer of a torus in G, S the connected center of U and $k = \dim S$. Then, for a suitable ordering $\mathcal{S}$, there are $l - k$ simple roots a_i $(1 \leqq i \leqq l - k)$ vanishing on S and such that the roots of U are exactly the roots of G which are linear combinations of the a_i $(1 \leqq i \leqq l - k)$.*

The roots of U are those of G which vanish on S; since the semi-simple part of U has rank $l - k$, U has $l - k$ independent roots. We consider in the dual space V_T^* of the universal covering V_T of T the lexicographic order which is associated to a base whose first k elements span the covering V_S of S. It is then clear that if a sum of positive linear forms b_i with strictly positive coefficients vanishes on V_S, so does each b_i; the lemma follows readily from this and from the fact that U has $l-k$ linearly independent roots.

Remark. In the ordering $\mathcal{O}$, the complementary roots are linear combinations of the a_j's with at least one of the k last ones appearing with a non-zero coefficient. Therefore, if the sum $a+b$ of a root a of U and of a complementary root b is a root, then it must be a complementary root. Also, the set of positive complementary roots is closed.

13.7. *Number of invariant complex structures.* In this section, we assume G/U to be homogeneous complex; U is then the centralizer of a torus by 13.5, and we keep the notations of 13.6.

PROPOSITION. *Let Θ be a system of positive roots of U. The roots of an invariant complex structure form a closed system Ψ such that $\Theta \cup \Psi$ is a positive system of roots for G. Conversely, a closed set Ψ of complementary roots such that $\Theta \cup \Psi$ is the set of positive roots of G for a suitable ordering is the system of roots of an invariant complex structure of G/U.*

Let Ψ be the root system of an invariant complex structure $\mathcal{C}$. Then (12.4) Ψ is closed and is contained in a system Φ of positive roots of G. Φ is necessarily of the form $\Theta' \cup \Psi$, where Θ' is a system of positive roots for U. There exists, therefore, $w \in W(U)$ which carries Θ' onto Θ; since w leaves Ψ invariant (remark in 13.4), it carries $\Theta' \cup \Psi$ onto $\Theta \cup \Psi$, and the latter is also a positive system.

Let now Ψ be a closed system of complementary roots such that $\Theta \cup \Psi$ is the set of positive roots relative to an ordering $\mathcal{O}'$. The remark in 13.6 and the fact that Ψ is closed show that if $a \in \Theta$ is a sum of two positive roots for $\mathcal{O}'$, then these two roots also belong to Θ; this means that the simple roots of Θ, considered as a positive system for U, are also simple for $\mathcal{O}'$. Let then a_j $(1 \leqq j \leqq l)$ be the simple roots of $\mathcal{O}'$, with $a_j \in \Theta$ for $j \leqq l-k$; the elements of Θ (resp. Ψ) are then linear combinations with positive coefficients of $a_1, \cdots, a_{l-k}$ (resp. $a_1, \cdots, a_l$, where at least one a_j $(j > l-k)$ has a non-vanishing coefficient). This implies first that $\Theta \cup -\Theta \cup \Psi$ is closed and second that there is an $s \in S$ such that $0 < b(s) < \frac{1}{2}$ for all $b \in \Psi$; thus the map of $(G/U)_0 \cong \mathfrak{g}/\mathfrak{u}$ onto itself, defined by $\operatorname{Ad} s$, has no real eigenvalues and the complex structure attached to it by the rule of 12.1 has the root system Ψ. Since s commutes with U, this structure is invariant under the isotropy representation, and hence, by (12.4), gives an invariant complex structure on G/U.

13.8. PROPOSITION. *Let G/U be homogeneous complex, let k be the dimension of the center of U, and let l be the rank of G. If $k=1$ (resp. $k=l$, i.e., $U=T$), then the number of invariant complex structures is equal to two (resp. the order of $W(G)$). Given two of them, there is a homeomorphism of G/U induced from an (resp. inner) automorphism of G leaving U invariant and carrying one onto the other.*

Let $k=l$. Then in the notations of 13.7, Θ is empty and the invariant complex structures are in 1-1 correspondence with the different systems of positive roots of G, by 13.7 (or directly by 4.9 and 12.4). Since $W(G)$ operates transitively on the set of systems of positive roots, it is obvious by the remark of 13.4 that the inner automorphisms of G defined by the elements of the normalizer of T induce homeomorphisms of G/T which permute transitively the invariant complex structures.

Now let $k=1$. We first take an ordering $\mathcal{S}$ having the properties mentioned in 13.6. Then the set of positive complementary roots Ψ defines an invariant complex structure by 13.7. Let Ψ' be the root system of another invariant complex structure. As in 13.7, we denote by Θ the set of roots of U which are positive for $\mathcal{S}$ and by a_l the simple root of $\mathcal{S}$ not belonging to Θ; $\Psi' \cup \Theta$ is the set of positive roots for some ordering $\mathcal{S}'$, and the proof of Proposition 13.7 shows that $a_1, \cdots, a_{l-1}$ are also simple for $\mathcal{S}'$. If $a_l \in \Psi'$, then $\Psi' \cup \Theta$ contains all simple roots of $\mathcal{S}'$, and hence $\Psi = \Psi'$. Let now $-a_l \in \Psi'$ and let a'_l be the l-th simple root of $\mathcal{S}'$; $-a_l$ is a linear combination with positive coefficients of $a_1, \cdots, a_{l-1}, a'_l$, and therefore, if we express a'_l as a linear combination of $a_1, \cdots, a_l$, then the root a_l must have coefficient -1. But then the elements of Ψ' which are combinations with positive coefficients of $a_1, \cdots, a_{l-1}, a'_l$, where the last coefficient is $\neq 0$, must also have at least one negative coefficient when expressed as linear combinations of $a_1, \cdots, a_l$; this means that they are negative for $\mathcal{S}$, and therefore that $\Psi' = -\Psi$. Thus we have only two invariant complex structures.

It is known (see [23] or Gantmacher, Rec. Math. Moscou 47 (1939), 101-144) that any automorphism of $\mathfrak{t}$ permuting the roots extends to an automorphism of $\mathfrak{g}$. In particular, there is an automorphism σ carrying each root into its opposite; since we may assume here G to be simply connected (10.1), σ also defines an automorphism of G leaving T invariant; it maps Ψ onto $-\Psi$ and leaves invariant the set of roots of U. Therefore σ leaves U

invariant and defines a homeomorphism of G/U carrying the complex structure with roots Ψ onto the complex structure with roots $-\Psi$.

Remarks. 1) The argument which ends the preceding proof shows more generally the following: let Ψ, Ψ' be the root systems of two invariant complex structures $\mathscr{C}$, $\mathscr{C}'$ on G/U. If there is an automorphism of V_T carrying Ψ onto Ψ' and leaving the root system of U invariant, then $\mathscr{C}$, $\mathscr{C}'$ are equivalent under a differentiable homeomorphism of G/U, which is induced from an automorphism of G leaving U invariant.

2) If Ψ is the set of roots of an invariant complex structure $\mathscr{C}$, then $-\Psi$ is clearly the root system of the "bar structure" or conjugate of Ψ, that is, of the structure in which the vectors of type $(1,0)$ are those of type $(0,1)$ for $\mathscr{C}$. Thus the last part of the above proof shows that on G/U an invariant complex structure and its conjugate are equivalent under an automorphism of G. In the case $\boldsymbol{P}_{n-1}(C)=\boldsymbol{U}(n)/\boldsymbol{U}(n-1)\times\boldsymbol{U}(1)$, the automorphism may be taken as complex conjugation and therefore has to be an outer automorphism for $n\geqq 3$.

3) The case $k=1$ in 13.8 includes the hermitian symmetric spaces for which our assertion has already been noticed by I. Satake, "A remark on bounded symmetric domains," Sci. Papers Coll. Ed. Gen. Univ. Tokyo 3 (1953), 131-144).

13.9. *Examples of inequivalent structures.* There are cases in which G/U carries at least two invariant complex structures which are not equivalent under a differentiable homeomorphism. For instance, take $G=\boldsymbol{U}(4)$, $U=\boldsymbol{U}(2)\times\boldsymbol{U}(1)\times\boldsymbol{U}(1)$, embedded in the standard fashion. With respect to the standard maximal torus, the roots of $\boldsymbol{U}(4)$ are $\pm(x_i-x_j)$, $(1\leqq i<j\leqq 4)$, and those of U are $\pm(x_1-x_2)$. Let $\mathscr{S}_1$ (resp. $\mathscr{S}_2$) be the ordering defined by $x_4>x_1>x_2>x_3>0$ (resp. $x_1>x_2>x_3>x_4>0$). Then by 13.7, the set Ψ_1 (resp. Ψ_2) formed by x_4-x_1, x_4-x_2, x_4-x_3, x_1-x_3, x_2-x_3 (resp. x_1-x_3, x_1-x_4, x_2-x_3, x_2-x_4, x_3-x_4) is the root system of an invariant complex structure $\mathscr{C}_1$ (resp. $\mathscr{C}_2$). The image in $H^2(\boldsymbol{U}(4)/\boldsymbol{T},\boldsymbol{Z})$ of the first Chern class of $\mathscr{C}_1$ (resp. $\mathscr{C}_2$) is, by 10.8, equal to $3(x_4-x_3)$ (resp. $2x_1+2x_2-x_3-3x_4$). Now $\boldsymbol{U}(4)/\boldsymbol{T}=\boldsymbol{SU}(4)/\boldsymbol{T}'$ where $\boldsymbol{T}'=\boldsymbol{T}\cap\boldsymbol{SU}(4)$ is a maximal torus of $\boldsymbol{SU}(4)$. The inclusion map of $\boldsymbol{T}'$ in $\boldsymbol{T}$ identifies $H^1(\boldsymbol{T}',\boldsymbol{Z})$ with the quotient of $H^1(\boldsymbol{T},\boldsymbol{Z})$ by $\boldsymbol{Z}\cdot(x_1+x_2+x_3+x_4)$; since $\boldsymbol{SU}(4)$ is simply connected, the transgression is an isomorphism of $H^1(\boldsymbol{T}',\boldsymbol{Z})$ on $H^2(\boldsymbol{SU}(4)/\boldsymbol{T}',\boldsymbol{Z})$. It follows then that the first Chern class of $\mathscr{C}_1$ (resp. $\mathscr{C}_2$) is divisible (resp. not divisible) by 3. Hence $\mathscr{C}_1$ and $\mathscr{C}_2$ are not equivalent under a differentiable homeomorphism of G/U. Moreover it will be shown in Section 24.14 that the Chern numbers c_1^5 of $\mathcal{B}_1$ and $\mathcal{B}_2$ are equal to 4860 and 4500 respectively.

The following observation leads to other examples:

PROPOSITION. *Assume that G/U carries two invariant homogeneous structures $\mathcal{B}$, $\mathcal{B}'$ with root systems Ψ, Ψ', and that G^c is the greatest connected group of automorphisms of $\mathcal{B}$ and of $\mathcal{B}'$. Then $\mathcal{B}$ and $\mathcal{B}'$ are equivalent under a differentiable homeomorphism of G/U if and only if there is a linear transformation α of $\mathfrak{t}$ leaving the root system of U invariant and carrying Ψ onto Ψ'.*

The "if" part follows from Remark 1) in 13.8.

Let now β be a differentiable homeomorphism of G/U carrying $\mathcal{B}$ onto $\mathcal{B}'$. By the assumption on G^c, β defines an automorphism of G^c. Using homogeneity and the facts recalled in 14.3, it is then seen that $\mathcal{B}$ and $\mathcal{B}'$ are also equivalent under a homeomorphism γ which is induced from an automorphism of G^c leaving U^c, T^c invariant. Since γ permutes the roots of $\mathfrak{g}^c$ with respect to $\mathfrak{t}^c$, and since $\mathfrak{t}$ is characterized as the subset of $\mathfrak{t}^c$ on which the roots are real valued, γ leaves $\mathfrak{t}$ invariant, and its restriction to $\mathfrak{t}$ is the desired α. Q. E. D.

According to Bott (unpublished), G^c satisfies our assumption, for instance, if $G = \boldsymbol{E}_7, \boldsymbol{E}_8$. Moreover, $\boldsymbol{E}_7, \boldsymbol{E}_8$ have no outer automorphisms, hence the automorphisms of $\mathfrak{t}$ keeping the root system of G invariant are just those of the Weyl group. Let now a, b be two different simple roots with respect to an ordering $\mathcal{S}$ and let $w \in W(G)$ be a transformation carrying b onto a. (This exists because the roots of $\boldsymbol{E}_7$ or $\boldsymbol{E}_8$ all have the same length and $W(G)$ is known to be transitive on a set of roots of the same length.)

Let Φ be the set of positive roots for $\mathcal{S}$, and $\Psi = \Phi - a$, $\Psi' = w(\Phi - b)$. The symmetry to $a = 0$ carries Φ onto $-a \cup \Psi$ (see the proof of 3.1). Therefore, if there existed an α carrying $\pm a$ onto itself and Ψ onto Ψ', there would also be a $w' \in W(G)$ carrying a onto b and leaving Φ invariant, but this contradicts the fact that $W(G)$ is simply transitive on the Weyl chambers (2.7). Now $\pm a$ is the set of roots of the centralizer U of the singular torus defined by $a = 0$. Thus, by our criterion, Ψ and Ψ' are the root systems of two invariant complex structures on G/U which are not equivalent under a differentiable homeomorphism. A similar discussion would also show that the complex structures on $\boldsymbol{U}(4)/\boldsymbol{U}(2) \times \boldsymbol{U}(1) \times \boldsymbol{U}(1)$ discussed above are not equivalent.

14. Complex Lie groups, embeddings, representations, invariant differential forms. We collect here some results to be used in the sequel. For more details about the facts mentioned without proofs in 14.3, 14.4 or about related questions, see [5], [7a], Goto "On algebraic homogeneous spaces," *Amer. Jour. Math.* 76 (1954), 811-818, J. Tits, "Sur certaines classes d'espaces homogènes de groupes de Lie," *Mém. Acad. Royale Belgique* 29 (1955), Chapitre III.

14.1. *Notations.* G is semi-simple and simply connected, $\mathcal{S}$ is an ordering of the roots with respect to T, and $a_1, \cdots, a_l$ are the simple roots for $\mathcal{S}$. If I is a (possibly empty) proper subset of $[1, l]$, we denote by U_I the centralizer of the torus S_I defined by $a_i(t) = 0$ $(i \in I, t \in T)$ and put $M_I = G/U_I$. We consider it to be endowed with the invariant complex structure $\mathcal{C}_I$ defined by the set Ψ_I or Ψ of *positive complementary roots* (whose existence follows from 13.7). U_I' is the semi-simple part of U_I. Thus we have $U_I = S_I \cdot U_I'$ with $S_I \cap U_I'$ finite.

Remark. Let G be a compact connected Lie group and G_1, G', U, U_1, U' be as in 10.1. Then $G/U = G'/U' = G_1/U_1$. By a result of Hopf (see e.g. [23, Exp. XXI]), the centralizer of a toral subgroup in a compact connected Lie group is connected; hence, if one of U, U', U_1 is centralizer of a torus, so are the other two. Thus the assumption G semi-simple and simply connected made in § 14, which allows one to avoid some slight irrelevant technical complications, is no real restriction, and the results of this paragraph are valid, with little or no modification, in the general case. In particular, in 14.4 one has to consider then the representations of the group $\bar{G}$ mentioned in 2.9.

14.2. The natural map $\nu_I \colon G/T \to G/U_I$ is the projection in the fibering $(G/T, G/U_I, U_I/T)$; the spaces $G/T, G/U_I, U_I/T$ have no torsion and have vanishing odd dimensional Betti numbers ([5] or R. Bott, *Bull. Soc. Math. France* 84 (1956), 251-81). Therefore [2, § 4], for any commutative group A of coefficients, the fibre is totally non homologous to zero, ν_I^* is injective, $\nu_I^*(H^2(G/U_I, A))$ is the kernel of the map of $H^2(G/T, A)$ into $H^2(U_I/T, A)$ induced by inclusion. It follows that $\nu_I^*(H^2(G/U_I, A)$ is a direct summand of $H^2(G/T, A)$; also, since the transgression in $(G, G/U_I, U_I)$ is an isomorphism of $H^1(U_I, \mathbf{Z})$ onto $H^2(G/U_I, \mathbf{Z})$, the former group is free abelian.

LEMMA. *Let A be a principal ideal ring. Then ν_I^* is an isomorphism of $H^2(G/U_I, A)$ onto the submodule of $H^2(G/T, A)$ formed by the elements orthogonal to the a_i's $(i \in I)$, that is, which is spanned by the fundamental weights ϖ_i's $(i \notin I)$.*

By the above and the universal coefficient formula, it is enough to prove the lemma for $A = \mathbf{Z}$. The fundamental weights ϖ_i $(1 \leqq i \leqq \operatorname{rank} G)$, form a basis of $H^1(T, \mathbf{Z})$, (see 3.4), hence of $H^2(G/T, \mathbf{Z})$, and the subgroup B_I spanned by the ϖ_i's $(i \notin I)$ is a direct summand whose rank equals the dimension of S_I.

The group $T' = T \cap U_I'$ is a maximal torus of U_I', whose covering in the universal covering V_T of T is spanned by the contravariant images of the a_i $(i \in I)$. Since U_I' is semi-simple and U_I is locally isomorphic to the product $S_I \times U_I'$, the map $H_1(S_I, \mathbf{R}) \rightarrow H_1(U_I, \mathbf{R})$, (resp. $H_1(T', \mathbf{R}) \rightarrow H_1(U_I, \mathbf{R})$), induced by inclusion, is an isomorphism (resp. has zero image). Since $H^1(U_I, \mathbf{Z})$ is free, it follows immediately that $\alpha^* : H^1(U_I, \mathbf{Z}) \rightarrow H^1(T, \mathbf{Z})$ is injective, with its image contained in B_I, and of finite index in B_I, where α is the inclusion of T in U_I.

The projection ν_I defines a representation of the fibering $(G, G/T, T)$ into $(G, G/U_I, U_I)$, whose restriction to a fibre is α. Therefore, using transgression, we see that the image of ν_I^* is a subgroup of finite index of B_I. But we have already shown that it is a direct summand, whence the lemma.

Remark. By transgression, we also see that α^* identifies $H^1(U_I, \mathbf{Z})$ with B_I.

14.3. *Complexification.* G^c denotes the complex Lie group containing G, with Lie algebra $\mathfrak{g}^c$, whose existence and uniqueness up to an isomorphism is well known. We use the notation of §§ 1, 12 and, moreover, put

$$\mathfrak{p}_I = \mathfrak{u}_I{}^c + \sum_{-b \in \Psi} \mathfrak{b}_b.$$

It is a subalgebra which generates a closed, connected, complex analytic subgroup P_I of G^c, equal to its normalizer, such that $P_I \cap G = U_I$; it follows then that G is transitive on G^c/P_I and that there is a natural identification of G/U_I with G^c/P_I which carries $\mathcal{J}_I$ onto the quotient complex structure, as defined in the theory of complex Lie groups (see e.g. [7a]). If, in particular, I is empty, then $\mathfrak{b} = \mathfrak{p}_I$ is solvable and $G^c/B = G/T$, where $B = P_I$.

14.4. *Representations and embeddings.* Let $\mathcal{S}^-$ be the ordering of the roots which is opposite to $\mathcal{S}$, that is, which has the negative roots of $\mathcal{S}$ as positive roots. The highest weights of the irreducible representations of G with respect to $\mathcal{S}^-$ are then the opposite of the highest weights in the order $\mathcal{S}$. If Γ has highest weight ϖ for $\mathcal{S}$ and Γ' highest weight $-\varpi$ for $\mathcal{S}^-$, then Γ' is the contragredient representation to Γ, and its weights are the opposite of those of Γ.

Let Γ be an irreducible representation of degree $q+1$,

$$\varpi = c_1\varpi_1 + \cdots + c_l\varpi_l$$

its highest weight in the ordering $\mathcal{S}$, $\check{\Gamma}$ the contragredient representation, $\check{\Gamma}'$ and Γ' the associated representations by means of projective transformations in $\boldsymbol{P}_q(C)$. Let V be a representation space for $\check{\Gamma}$ and π be the projection of $V-0$ on $\boldsymbol{P}_q(C)$. There is in V exactly one 1-dimensional subspace W which is invariant under B, and we have

$$\check{\Gamma}(t)(x) = \exp[-2\pi i\varpi(t)]\cdot x, \qquad (t\in T^c, x\in W).$$

$x' = \pi(W-0)$ is then the unique point of $\boldsymbol{P}_q(C)$ fixed under $\check{\Gamma}'(B)$.

We say that M_I is *associated* (resp. *strictly associated*) to Γ if $c_i = 0$ for $i\in I$ (resp. and, moreover, if $c_j \neq 0$ for $j\notin I$). If M_I is associated (resp. strictly associated) to Γ, then the map $\phi\colon g\to\check{\Gamma}'(g)\cdot x'$ induces a holomorphic (resp. bijective and bi-holomorphic) map β_I of M_I onto a projective non-singular variety M_Γ. In particular, each irreducible representation yields a holomorphic map β_2 of G/T into some projective space. Since a given M_I is strictly associated to infinitely many representations, it therefore admits projective embeddings.

The cone $\pi^{-1}(M_\Gamma)$ over M_Γ is, in the obvious way, a $\boldsymbol{C}^*$-bundle η over M_Γ; on the other hand, let N be the subgroup of B whose Lie algebra over $\boldsymbol{C}$ is spanned by the $\mathfrak{v}_a$ ($a<0$ for $\mathcal{S}$). N is the commutator subgroup of B, and $B/N \cong T^c$. The quotient G^c/N can be considered as the total space of a principal T^c-bundle $\xi = (G^c/N, G^c/B, T^c)$. If γ is the representation of T^c with character $\exp(-2\pi i\varpi)$, it is then easily seen that β_2 induces a γ-homomorphism of ξ on η. Therefore, by 10.4, $\varpi = -\beta_2^*(c_1(\eta))$. It follows from this and from 14.2 that if M_I is associated to Γ, then $-\varpi$ may be identified with an element of $H^2(M_I, \boldsymbol{Z})$ which is the Chern class of the bundle over M_I induced from η by $\beta_I\colon M_I\to M_\Gamma$. But $c_1(\eta)$ is $-e^*$, where e^* is the dual of the homology class containing a hyperplane section of M_I (see § 29). Thus ϖ is the dual of the homology class of a divisor on M_I, namely, the inverse image of a hyperplane section of M_Γ. It may be shown [7a] that the inverse images of the hyperplane sections of M_Γ form a complete linear system on M_I, and that this system is the only one on which the natural representation of G is Γ'.

14.5. *Positive classes.* Since we want to use some facts about complex Lie algebras, we now identify V_T with its tangent space $\mathfrak{t}$ at e, and assume the invariant metric to be the restriction of $-K$, where K is the Killing form. The roots of $\mathfrak{g}^c$ with respect to $\mathfrak{t}^c$ in the sense of infinitesimal theory are then the forms $2\pi i a$, where a runs through the roots as defined in this paper (or, more precisely, through their extensions to $\mathfrak{t}^c$, since they were originally defined on V_T or $\mathfrak{t}$). If a is a linear form on $\mathfrak{t}^c$, we denote by h_a its contravariant representative with respect to $-K$; if a is real valued on $\mathfrak{t}$, then $h_a \in \mathfrak{t}$. It is known (see, for instance, [23], Exp. 10, 11) that we can find $e_a \in \mathfrak{v}_a$ with the following properties:

$$(1) \qquad [e_a, e_{-a}] = 2\pi i h_a, \qquad K(e_a, e_{-a}) = -1,$$

$\mathfrak{g}$ is spanned over the reals by $\mathfrak{t}$ and the vectors $e_a + e_{-a}$, $i(e_a - e_{-a})$, and the Killing form is the direct sum

$$K = K_1 - \sum_{a>0} x_a x_{-a},$$

where K_1 is the restriction of K to $\mathfrak{t}^c$ and the x_a, x_{-a} form the dual base to (e_a, e_{-a}).

Finally, we recall that if X, Y are left-invariant vector fields and ω is a left-invariant 1-form on a Lie group H, then

$$(2) \qquad d\omega(X, Y) = -\omega([X, Y]) \qquad ([X, Y] = X \cdot Y - Y \cdot X)$$

(see e.g. Chevalley, *Theory of Lie groups I*, Princeton, Chap. V, § 4; it is there stated for real Lie groups, but the proof is also valid in the complex case).

Let us denote by ω_a the left-invariant 1-form on G^c whose restriction to $\mathfrak{g}^c$ is annihilated by $\mathfrak{t}^c$ and which is such that $\omega_a(e_b) = 1$ if $a = b$ and is zero if $a \neq b$. A straightforward computation using (1), (2) and 12.2 yields then the

LEMMA. *Let η_b be the left-invariant* 1-*form on G^c whose restriction to $\mathfrak{g}^c$ is zero on $\sum \mathfrak{v}_a$ and which induces the linear form b on $\mathfrak{t}^c$. Then*

$$(3) \qquad d\eta_b = -2\pi i \sum_{a>0} (b, a)\, \omega_a \wedge \omega_{-a}.$$

We are interested only in the case where b is real valued on $\mathfrak{t}$; then (b, a) is also real valued. Assume now that b is orthogonal to the roots a_i $(i \in I)$, i.e., that $h_b \in \mathfrak{s}_I$. Then

$$(4) \qquad d\eta_b = -2\pi i \sum_{a \in \Psi_I} (b, a)\, \omega_a \wedge \omega_{-a}.$$

The restriction $\eta_{b|G}$ of η_b to G is left-invariant. By (4), $d\eta_b$ is zero on $\mathfrak{u}$, and hence, by invariance, it vanishes on U; thus $\eta_{b|U}$ and, a fortiori, $\eta_{b|T}$ are closed. Since $\eta_{b|T}$ is clearly in the class $b \in H^1(T, \boldsymbol{R})$, it follows by 14.2

that $\eta_b|_U$ represents the element of $H^1(U,\mathbf{R})$ which we have identified with b. We want to show that $d\eta_b|_G$ is the inverse image of a 2-form on M_I; for this, it is necessary and sufficient that the 2-form defined by $d\eta_b$ on $\mathfrak{g}$ vanishes whenever one of the arguments is in $\mathfrak{u}_I$ and is invariant under $\mathrm{Ad}_{\mathfrak{g}}\,U_I$ (see e.g. Chevalley-Eilenberg, Trans. A. M. S. 63 (1948), 85-124, Theorem 13.1). The first property is obvious from (4); as to the second, we may argue as follows: by (4), we have only to show that the restriction of $d\eta_b$ *to* $\sum_{\mathfrak{b}\in\Psi}\mathfrak{b}$ is invariant under the linear isotropy group $\tilde{U}$. From the properties of the Killing form recalled above, we see that if we take in $\mathfrak{b}$ the real and imaginary parts of x_b as coordinates, then the Killing form is the negative unit form, and therefore, the isotropy group $\tilde{U}$ is orthogonal; this means that $d\eta_b$ is invariant under $\tilde{U}$ if its matrix commutes with $\tilde{U}$. But it follows from (4) and 12.2 that this matrix is equal to the restriction of the matrix of $\mathrm{ad}_{\mathfrak{g}}\,h_b$. Since $h_b\in\mathfrak{s}_I$, it centralizes $\mathfrak{u}$, and $\mathrm{ad}_{\mathfrak{g}}\,h_b$ does commute with $\mathrm{Ad}_{\mathfrak{g}}\,U$.

By the foregoing and by the definition of transgression, $d\eta_b|_G$ may be identified with a closed 2-form on G/U_I belonging to the image of $b\in H^1(U,\mathbf{R})$ under transgression; in view of the conventions made in 10.1, this form represents the cohomology class which has been identified with $-b$. Moreover, by the definition of the complex structure $\mathscr{B}_I$ on M_I, the $\mathfrak{v}_a$ $(a\in\Psi_I)$, span the subspace of $M_I\otimes\mathbf{C}$ which contains the differentials of local holomorphic functions, and we have $\omega_{-a}=\overline{\omega}_a$ in the standard notations. Thus we have shown the following:

14.6. PROPOSITION. *We keep the notations of* 14.1, 14.2. *Let b be a linear form on V_T orthogonal to the simple roots a_i $(i\in I)$. Then the element of $H^2(G/U_I,\mathbf{R})$ identified with b in* 14.2 *contains the invariant 2-form of type* (1,1)

$$\omega=2\pi i\sum_{a\in\Psi_I}(b,a)\,\omega_a\wedge\overline{\omega}_a. \tag{5}$$

ω is the imaginary of the hermitian form

$$4\pi\sum_{a\in\Psi}(b,a)\,\omega_a\cdot\overline{\omega}_a\ \text{(symmetric product)}. \tag{6}$$

A 2-dimensional complex cohomology class on a complex manifold M is *positive in the sense of* Kodaira if it contains the imaginary part of a positive non-degenerate hermitian metric, which is then necessarily kählerian. From (5), (6) and the remark in 13.6, we get:

14.7. COROLLARY. *b is positive in the sense of Kodaira if $(b,a)>0$ for $a\in\Psi_I$, that is, if $(b,a_i)>0$ for $i\notin I$.*

This is in agreement with the fact (14.4) that when b is the highest weight of an irreducible representation Γ to which M_I is strictly associated, then it is dual to the class of a hyperplane section in the projective embedding provided by the representation $\check{\Gamma}$.

14.8. COROLLARY. *The first Chern class c_1 of the tangent bundle to M_I is positive.*

c_1 is the sum of the positive complementary roots (10.7) and, by 13.6, these are the linear combinations of the simple roots in which at least one a_i with $i \notin I$ has a strictly positive coefficient. Thus, if $a \in \Psi_I$, its transform, by the symmetry to the plane $a_i = 0$ $(i \in I)$ belongs to Ψ_I. Since $(a_i, S_i a + a) = 0$, it follows that $(a_i, c_1) = 0$. This is also a consequence of 14.2.

In view of (5), (6), we have to show that if $a \in \Psi$, then $(a, c_1) > 0$. Let $b \in \Psi$ and assume that $(a, b) < 0$. Then (§2)

$$b, b + a, b + 2a, \cdots, b + ka \qquad (k = -2(a,b)(a,a)^{-1}) \tag{7}$$

are roots of G and, in fact, belong to Ψ, since the latter is a closed system (13.7). We have $(a, b + ka) = (a,a)k/2 > 0$ and

$$(a, b + b + a + \cdots + b + ka) = (k+1)(a,b) + (a,a)k \cdot (k+1)/2 = 0.$$

From this we deduce readily that we may represent Ψ as a union of disjoint subsets Ψ_j, where Ψ_j consists either of one root b with $(a, b) \geqq 0$ or of a string of type (7), whose sum is orthogonal to a; in the first category we have the set consisting of a itself, and hence, finally, $(a, c_1) > 0$.

14.9. Using some properties of the constants of structure of $\mathfrak{g}^c$, one can show that 14.6 gives all invariant 2-forms on M_I, as indicated in [5]; this implies that the condition of 14.7 is also necessary for b to be positive as will also follow from § 24.

14.10. We recall that for a kählerian compact manifold M, the d- and the $\bar{\partial}$-cohomology are identical, and that $H^i(M, \boldsymbol{C})$ is a direct sum of subspaces $H^{p,q}(M)$, $(p + q = i)$, where $H^{p,q}$ is the space of i-dimensional cohomology classes which can be represented by exterior differential forms of type (p, q). This applies, in particular, to the projective variety G/U_I.

PROPOSITION. *In the previous notations, we have $H^{2i+1}(M_I, \boldsymbol{C}) = 0$ and $H^{2i}(M_I, \boldsymbol{C}) = H^{i,i}(M_I)$ for all $i \geqq 0$.*

For the first assertion, see [2, Théorème 26.1].

As remarked in 14.2, the projection ν_I of G/T onto G/U_I induces an injective homomorphism of $H^*(G/U_I, \boldsymbol{C})$ in $H^*(G/T, \boldsymbol{C})$. This map is also holomorphic with respect to the complex structures on G/T and G/U_I defined by the positive complementary roots, because, in the notations of 14.3, it can be identified with the projection of G^c/B onto G^c/P_I, both spaces being endowed with the natural quotient complex structures. Thus $\nu_I{}^*$ identifies $H^{p,q}(M_I)$ with a subpace of $H^{p,q}(G/T, \boldsymbol{C})$, and it suffices to prove our contention for G/T. Since $H^*(G/T, \boldsymbol{C})$ is generated by the unit and its 2-dimensional classes [2, § 26], it is enough to show that $H^2(G/T, \boldsymbol{C}) = H^{1,1}(G/T)$, but this follows from 14.6.

Chapter V. Special Cases.

15. Projective spaces.

15.1. *Complex projective spaces.* We wish to apply Theorem 10.8 to the case where $G = \boldsymbol{U}(q)$ and $U = \boldsymbol{U}(1) \times \boldsymbol{U}(q-1)$ and $G/U = \boldsymbol{P}_{q-1}(\boldsymbol{C})$, $(q \geqq 2)$. The imbedding of U in G is the usual one; namely, as follows: $\boldsymbol{U}(q)$ is the group of unitary matrices and $\boldsymbol{U}(1) \times \boldsymbol{U}(q-1)$ is the group of $q \times q$-matrices of the form

$$\begin{pmatrix} a' & 0 \\ 0 & A'' \end{pmatrix},$$

where $a' \in \boldsymbol{U}(1)$ and $A'' \in \boldsymbol{U}(q-1)$, which is a subgroup of maximal rank of G. Let $\boldsymbol{T}$ be the standard maximal torus of diagonal unitary matrices

$$\begin{bmatrix} e^{2\pi i x_1} & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & e^{2\pi i x_q} \end{bmatrix}.$$

$\boldsymbol{T}$ is contained in $\boldsymbol{U}(1) \times \boldsymbol{U}(q-1)$ and plays the role of S in Theorem 10.7. The coordinates $x_1, \cdots, x_q$ are integral linear forms on V_T (see 1.2 and 10.1), and the roots of $\boldsymbol{U}(q)$ with respect to $\boldsymbol{T}$ are $\pm (x_j - x_k)$, where $1 \leqq j < k \leqq q$. The roots of $\boldsymbol{U}(1) \times \boldsymbol{U}(q-1)$ are $\pm (x_j - x_k)$ with $2 \leqq j < k \leqq q$. Hence the roots of $\boldsymbol{U}(q)$ complementary to $\boldsymbol{U}(1) \times \boldsymbol{U}(q-1)$ are $\pm (x_1 - x_j)$ with $2 \leqq j \leqq q$.

The usual invariant complex structure of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$ is given by regarding $\boldsymbol{P}_{q-1}(C)$ as the space of the lines passing through the origin of $\boldsymbol{C}^q$. Let $\boldsymbol{GL}(q, \boldsymbol{C})$ operate in the usual way on $\boldsymbol{C}^q$ and thus on $\boldsymbol{P}_{q-1}(\boldsymbol{C})$. Let $\boldsymbol{GL}(1, q-1; \boldsymbol{C})$ be the subgroup of those elements of $\boldsymbol{GL}(q, C)$ which keep the point $(1, 0, \cdots, 0)$ of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$ fixed. Then

$$\boldsymbol{U}(q)/(\boldsymbol{U}(1)\times\boldsymbol{U}(q-1))=\boldsymbol{GL}(q,C)/\boldsymbol{GL}(1,q-1;C)=\boldsymbol{P}_{q-1}(\boldsymbol{C}).$$

Thus $\boldsymbol{P}_{q-1}(\boldsymbol{C})$ is represented as a quotient of complex Lie groups and is, therefore, endowed with an invariant structure which is just the usual one. The complex isotropy representation ι_c of this complex structure has the weights x_j-x_1 $(j=2,\cdots,q)$, which can be seen as follows: The element $(e^{2\pi i x_1},\cdots,e^{2\pi i x_q})$ of $\boldsymbol{T}$, when operating on the point $(1,z_2,\cdots,z_q)$ of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$, gives the point

$$(1,z_2e^{2\pi i(x_2-x_1)},\cdots,z_qe^{2\pi i(x_q-x_1)})$$

of $\boldsymbol{P}_{q-1}(C)$, which proves the desired result. We may remark here that $\boldsymbol{P}_{q-1}(C)$ admits exactly two invariant complex structures and these are complex conjugate to each other (see 13.8).

Let ξ be a principal $\boldsymbol{U}(q)$-bundle. We consider some associated fibre bundles and their projections according to the following diagram: Let ρ, σ be the natural projections

(1)
$$\begin{tikzcd} E_\xi/\boldsymbol{T} \arrow[r, "\rho"] & E_\xi/(\boldsymbol{U}(1)\times\boldsymbol{U}(q-1)) \arrow[r, "\sigma"] & B_\xi \end{tikzcd}$$

and $\pi=\sigma\circ\rho$. Let η be the real vector bundle along the fibres (7.4) of $(E_\xi/(\boldsymbol{U}(1)\times\boldsymbol{U}(q-1),B_\xi\boldsymbol{P}_{q-1}(\boldsymbol{C}))$ endowed with the complex structure η' coming from the usual invariant complex structure on $\boldsymbol{P}_{q-1}(\boldsymbol{C})$; i.e., η' is defined by the complex isotropy representation ι_c considered above. Then we have for the total Chern class of η'

$$\rho^*c(\eta')=\prod_{j=1}^{q}(1+x_j-x_1).$$

Now let $c_i\in H^{2i}(B_\xi,\boldsymbol{Z})$ be the Chern classes of ξ. Then we have (9.1)

$$\pi^*(1+c_1+c_2+\cdots+c_q)=(1+x_1)(1+x_2)\cdots(1+x_q).$$

Considering z as an indeterminate over $H^*(E_\xi/\boldsymbol{T},\boldsymbol{Z})$, we have the equation

$$z^q+z^{q-1}\pi^*(c_1)+\cdots+\pi^*(c_q)=(z+x_1)(z+x_2)\cdots(z+x_q).$$

Replacing z by $1-x_1$ gives

$$\rho^*c(\eta')=\prod_{j=1}^{q}(1+x_j-x_1)=\sum_{i=0}^{q}(1-x_1)^{q-i}\pi^*(c_i).$$

$x_1,x_2,\cdot\cdot,x_q$ are the first Chern classes of the q principal $\boldsymbol{U}(1)$-bundles $\xi_1,\cdots,\xi_q$, into which the principal bundle $(E_\xi,E_\xi/\boldsymbol{T},\boldsymbol{T})$ splits. The principal bundle $(E_\xi,E_\xi/(\boldsymbol{U}(1)\times\boldsymbol{U}(q-1)),\boldsymbol{U}(1)\times\boldsymbol{U}(q-1))$ splits into a principal $\boldsymbol{U}(1)$-bundle ξ' and a principal $\boldsymbol{U}(q-1)$-bundle ξ''. Obviously,

$\rho^*(\xi')$ is equivalent to ξ_1 and $\rho^*(\gamma_1) = x_1$, where γ_1 denotes the first Chern class of ξ'. Since $\pi^* = \rho^* \circ \sigma^*$ and since ρ^* is injective for integral cohomology, we get

$$c(\eta') = \sum_{i=0}^{q} (1-\gamma_1)^{q-i}\sigma^*(c_i). \tag{2}$$

Since $c_q(\eta') = 0$, we have

$$\sum_{i=0}^{q} (-\gamma_1)^{q-i}\sigma^*(c_i) = 0. \tag{3}$$

Once γ_1 is defined, the Chern classes of ξ are characterized by (3), a fact due to Hirsch (compare [11]).

To calculate the Chern class of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$, we now specialize to the case where $E_\xi = \boldsymbol{U}(q)$ and where B_ξ is a single point. Then η' is the tangent bundle of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$. Since $c_i = c_i(\xi) = 0$ for $i > 0$, we get

$$c(\eta') = c(\boldsymbol{P}_{q-1}(C)) = (1-\gamma_1)^q.$$

Now we observe that ξ' corresponds to the Hopf bundle; i.e., $(\boldsymbol{C}^q - \{0\}, \boldsymbol{P}_{q-1}(\boldsymbol{C}), \boldsymbol{C}^*)$ is the extension of ξ' with respect to the natural imbedding of $\boldsymbol{U}(1)$ in $\boldsymbol{C}^*$. Thus $-\gamma_1 = e^*$, where $e^* \in H^2(\boldsymbol{P}_{q-1}(\boldsymbol{C}), \boldsymbol{Z})$ is dual to the hyperplane of $\boldsymbol{P}_{q-1}(\boldsymbol{C})$ (see §29). Therefore

$$c(\boldsymbol{P}_{q-1}(\boldsymbol{C})) = (1+e^*)^q.$$

15.2. *Complex projective bundles.* In Sections 15.2 and 15.3, all cohomology groups are taken with real coefficients. The projective unitary group is defined by

$$\boldsymbol{PU}(q) = \boldsymbol{U}(q)/\boldsymbol{D},$$

where $\boldsymbol{D}$ is the 1-dimensional torus of scalar matrices of $\boldsymbol{U}(q)$. Let $\boldsymbol{T}^q$ be the maximal torus of diagonal matrices of $\boldsymbol{U}(q)$. Then $\tilde{\boldsymbol{T}}^{q-1} = \boldsymbol{T}^q/\boldsymbol{D}$ is a maximal torus of $\boldsymbol{PU}(q)$, and we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{D} \arrow[r] \arrow[d, "\mathrm{Id}"] & \boldsymbol{T}^q \arrow[r] \arrow[d] & \tilde{\boldsymbol{T}}^{q-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \boldsymbol{D} \arrow[r] & \boldsymbol{U}(q) \arrow[r, "\alpha"] & \boldsymbol{PU}(q) \arrow[r] & 0
\end{tikzcd} \tag{4}$$

which induces a commutative diagram for the classifying spaces (6.6)

$$\begin{tikzcd}
B_{\boldsymbol{D}} \arrow[r] \arrow[d, "\mathrm{Id}"] & B_{\boldsymbol{T}^q} \arrow[r] \arrow[d, "\pi"] & B_{\tilde{\boldsymbol{T}}^{q-1}} \arrow[d] \\
B_{\boldsymbol{D}} \arrow[r] & B_{\boldsymbol{U}(q)} \arrow[r, "\rho(\alpha)"] & B_{\boldsymbol{PU}(q)}
\end{tikzcd} \tag{5}$$

where the two horizontal lines come from the fibre bundles $(B_{T^q}, B_{\tilde{T}^{q-1}}, B_{\boldsymbol{D}})$ and $(B_{U(q)}, B_{PU(q)}, B_{\boldsymbol{D}})$, see [2]. Then, in the commutative diagram

$$\begin{tikzcd}
H^*(B_{T^q}) & H^*(B_{\tilde{T}^{q-1}}) \arrow[l] \\
H^*(B_{U(q)}) \arrow[u, "\pi^*"'] & H^*(B_{PU(q)}) \arrow[l, "\rho(\alpha)^*"'] \arrow[u]
\end{tikzcd} \tag{6}$$

which is induced by (5), all arrows indicate injections. If we denote by ξ the universal principal $\boldsymbol{U}(q)$-bundle and by $\tilde{\xi}$ the universal principal $\boldsymbol{PU}(q)$-bundle, then $\rho(\alpha)^*\tilde{\xi}$ is (up to equivalence) the α-extension of ξ. Let $x_1, \cdots, x_q$ be the first Chern classes (with real coefficients) of the q principal $\boldsymbol{U}(1)$-bundles into which $\pi^*\xi$ splits. Then

$$H^*(B_{T^q}) = \boldsymbol{R}[x_1, \cdots, x_q].$$

Using the Weyl group of $\boldsymbol{PU}(q)$ (which is isomorphic to that of $\boldsymbol{U}(q)$), it follows easily from diagram (6) that $\pi^*\rho(\alpha)^*H^*(B_{PU(q)})$ is the subring of those polynomials in $\boldsymbol{R}[x_1, \cdots, x_q]$ which are symmetric in $x_1, \cdots, x_q$ and invariant under the substitution $t\colon x_i \rightarrow x_i + b$, where b is an indeterminate. Roughly speaking, for a $\boldsymbol{PU}(q)$-bundle the Chern classes c_j (i.e., the elementary symmetric functions in the x_i) make no sense, but the polynomials in the c_j invariant under t do.

Now let $(L, X, \boldsymbol{P}_{q-1}(\boldsymbol{C}), \sigma)$ be a bundle with $\boldsymbol{PU}(q)$ as a structural group. It is known that σ^* maps $H^*(X)$ isomorphically in $H^*(L)$ (*real* cohomology) and that, for every element $\gamma \in H^2(L)$ whose restriction to the fibre equals the generator e^* of $H^2(\boldsymbol{P}_{q-1}(\boldsymbol{C}))$, there is (8.4) a relation

$$\gamma^q - \sigma^*(d_1)\gamma^{q-1} + \sigma^*(d_2)\gamma^{q-2} - \cdots + (-1)^q\sigma^*(d_q) = 0 \tag{7}$$

with uniquely determined elements $d_i \in H^{2i}(X)$ depending only on γ. Let η' be the complex vector bundle along the fibres of L. We recall that $\boldsymbol{P}_{q-1}(\boldsymbol{C}) = \boldsymbol{PU}(q)/((\boldsymbol{U}(1) \times \boldsymbol{U}(q-1))/\boldsymbol{D})$ and that the complex structure η' comes from the complex isotropy representation ι_c considered in 15.1 (ι_c is trivial on $\boldsymbol{D}$).

15.3. THEOREM. *The Chern class (with real coefficients) of the complex vector bundle η' along the fibres of a fibre bundle $(L, X, \boldsymbol{P}_{q-1}(C), \sigma)$ with $\boldsymbol{PU}(q)$ as structural group is given by the formula*

$$c(\eta') = \sum_{i=0}^{q} (1-\gamma)^{q-i}\sigma^*(d_i), \qquad (d_0 = 1), \tag{8}$$

where $\gamma \in H^2(L)$ is an arbitrary element whose restriction to the fibre gives the generator e^* and where the $d_i \in H^2(X)$ are defined by the relation (7).

For the proof, we introduce an indeterminate z. The polynomial

$$F(z)=\sum_{i=0}^{q} z^{q-i}\sigma^{*}(d_i), \quad (\text{see } (7)),$$

is then the unique element of $\sigma^{*}H^{*}(X)[z]$ which is a polynomial of degree q in z, has the unit 1 as the coefficient of z^{q}, and for which $F(-\gamma)$ vanishes. If $\tilde{\gamma}=\gamma+\sigma^{*}(b)$, where $b\in H^{2}(X)$; then $\tilde{F}(z)=F(z+\sigma^{*}(b))$ is the analogous unique polynomial with $\tilde{F}(-\tilde{\gamma})=0$. Since $F(1-\gamma)=\tilde{F}(1-\tilde{\gamma})$, the right side of (8) is independent of the choice of γ. Taking this into account, (2) and (3) of 15.1 yield our theorem for bundles whose structural groups can be α-reduced to $\boldsymbol{U}(q)$. Furthermore, we see that it is enough to prove the theorem for the universal principal $\boldsymbol{PU}(q)$-bundle $\tilde{\xi}$. Since the theorem is true for $\rho(\alpha)^{*}\tilde{\xi}$ (see (5)), it follows easily in full generality.

Theorem 15.3 was announced in the first note of [16].

15.4. *Real projective spaces.* In Section 15.4, all cohomology groups are taken with $\boldsymbol{Z}_2$ as coefficients. Let ξ be a principal $\boldsymbol{O}(q)$-bundle and η the vector bundle along the fibres of $(E_{\xi}/(\boldsymbol{O}(1)\times\boldsymbol{O}(q-1)), B_{\xi}, \boldsymbol{P}_{q-1}(\boldsymbol{R}))$. Let $\boldsymbol{Q}$ be the group of all diagonal matrices of $\boldsymbol{O}(q)$. Consider the maps

$$E_{\xi}/\boldsymbol{Q}\xrightarrow{\rho}E_{\xi}/(\boldsymbol{O}(1)\times\boldsymbol{O}(q-1))\xrightarrow{\sigma}B_{\xi},$$

and let w_i $(1\leqq i\leqq q)$ be the Stiefel-Whitney classes of ξ. Then we have

$$w(\eta)=\sum_{i=0}^{q}(1-\gamma_1)^{q-i}\sigma^{*}(w_i), \tag{9}$$

where γ_1 is the 1-dimensional characteristic class of the $\boldsymbol{O}(1)$-bundle over $E_{\xi}/(\boldsymbol{O}(1)\times\boldsymbol{O}(q-1))$. The class γ_1 induces on each fibre the generator of its cohomology ring. The proof uses 5.3 and 11.5 but is otherwise formally identical to that given in 15.1 (except that the x_i's are now 1-dimensional classes), and is therefore left to the reader. (9) implies the well-known fact that the Stiefel-Whitney class of $\boldsymbol{P}_{q-1}(\boldsymbol{R})$ equals $(1+a)^{q}$, where a is the generator of $H^{*}(\boldsymbol{P}_{q-1}(\boldsymbol{R}))$.

15.5. *The Pontrjagin classes of the quaternionic projective spaces.* The treatment of the quaternionic projective spaces

$$\boldsymbol{P}_{q-1}(\boldsymbol{K})=\boldsymbol{Sp}(q)/(\boldsymbol{Sp}(1)\times\boldsymbol{Sp}(q-1)), \qquad q\geqq 2,$$

is similar to the discussion in 15.1.

$\boldsymbol{Sp}(q)$ is the group of all unitary quaternionic $q\times q$-matrices. $\boldsymbol{Sp}(q)$ contains $\boldsymbol{U}(q)$, and $\boldsymbol{U}(q)$ contains the maximal torus $\boldsymbol{T}$ of 15.1 which is also maximal in $\boldsymbol{Sp}(q)$. When applying Theorem 10.7, we let ξ be the universal principal $\boldsymbol{Sp}(q)$-bundle. Putting

$$G=\boldsymbol{Sp}(q) \quad \text{and} \quad U=\boldsymbol{Sp}(1)\times\boldsymbol{Sp}(q-1),$$

we have the diagram

$$B_{\boldsymbol{T}}=E_\xi/\boldsymbol{T}\xrightarrow{\rho}B_U\xrightarrow{\sigma}B_G, \tag{10}$$

and the integral cohomology ring of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ has to be identified with $H^{**}(B_U,\boldsymbol{Z})$ (see 6.1) modulo the ideal $(I_G{}^+)^*$. As in 15.1, we have the elements $x_1,\cdots,x_q\in H^1(\boldsymbol{T},\boldsymbol{Z})$ which, via the negative transgression, are to be regarded as elements of $H^2(B_{\boldsymbol{T}},\boldsymbol{Z})$.

By means of (10), the cohomology ring $H^{**}(B_G,\boldsymbol{Z})$ will be considered as a subring of $H^{**}(B_U,\boldsymbol{Z})$, and $H^{**}(B_U,\boldsymbol{Z})$ as a subring of $H^{**}(B_{\boldsymbol{T}},\boldsymbol{Z})$. The latter ring will be identified with $\boldsymbol{Z}\{x_1,\cdots,x_q\}$. Thus $H^*(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z})$ is the quotient of

$$\boldsymbol{Z}\{x_1{}^2\}\otimes S\{x_2{}^2,\cdots,x_q{}^2\} \tag{11}$$

modulo the ideal $(I_G{}^+)^*$ which is generated by the symmetric power series in $x_1{}^2,\cdots,x_q{}^2$ without constant terms. (We use here essentially, that G and U have no torsion, see [2].)

We restrict ourselves to the calculation of the Pontrjagin classes of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$, i.e., of its tangent bundle. The more general case of the bundle along the fibres is left to the reader.

We do the calculations following a schema which will also be used in other cases.

Roots of $\boldsymbol{Sp}(q)$: $\pm x_i\pm x_j,\ \pm 2x_k \quad (1\leqq i<j\leqq q)$

Roots of $\boldsymbol{Sp}(1)\times\boldsymbol{Sp}(q-1)$: $\pm x_i\pm x_j,\ \pm 2x_k \quad (2\leqq i<j\leqq q)$

Complementary roots:

$$\pm(x_1-x_2,x_1-x_3,\cdots,x_1-x_q;x_1+x_2,x_1+x_3,\cdots,x_1+x_q).$$

We have

$$(1+x_2{}^2)(1+x_3{}^2)\cdots(1+x_q{}^2)=(1+x_1{}^2)^{-1} \qquad \operatorname{mod}(I_G{}^+)^*.$$

This shows that the r-th elementary symmetric function in the $x_j{}^2$ $(2\leqq j\leqq q)$ equals $(-1)^r x_1{}^{2r}$ $(\operatorname{mod}(I_G{}^+)^*)$ and that $x_1{}^2$ represents an element $u\in H^4(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z})$ which generates $H^*(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z})$; in particular, u is a generator of the infinite cyclic group $H^4(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z})$.

Introducing an indeterminate z, we have

$$\prod_{j=1}^{q}(z+x_j)(z-x_j)=z^{2q} \qquad \operatorname{mod}(I_G{}^+)^*.$$

Setting $z=1+x_1$, this yields

$$\prod_{j=2}^{q}(1+x_1+x_j)(1+x_1-x_j)=(1+x_1)^{2q}(1+2x_1)^{-1} \quad \operatorname{mod}(I_G{}^{+})^{*}. \tag{12}$$

Theorem 10.7 shows that the (integral) Pontrjagin class of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ is represented by the element

$$\prod_{j=2}^{q}(1+(x_1+x_j)^2)(1+(x_1-x_j)^2).$$

Taking into account that we are dealing with graded rings and that $x_1{}^2$ represents the generator u of $H^4(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z})$, we obtain from (12)

$$p(\boldsymbol{P}_{q-1}(\boldsymbol{K}))=(1+u)^{2q}(1+4u)^{-1}. \tag{13}$$

15.6. *Application.* Formula (13) implies, in particular, for the first (i.e., four-dimensional) Pontrjagin class of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ that

$$p_1=(2q-4)u.$$

p_1 is different from 0 for $q-1>1$.

Since $\phi^*(p_1)=p_1$ for all diffeomorphisms ϕ of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ onto itself, we see that, for $q-1>1$, there does not exist a diffeomorphism ϕ with $\phi^*(u)=-u$; i.e., for all ϕ, we have $\phi^*(u)=u$. In particular, all diffeomorphisms preserve orientation $(\phi^*(u^{q-1})=u^{q-1})$.

This fact on the orientation is obvious for $q-1\equiv 0\ (\operatorname{mod} 2)$ and aribtrary homeomorphisms of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ onto itself, since then

$$\phi^*(u)=\pm u \text{ implies } \phi^*(u^{q-1})=u^{q-1}.$$

15.7. *The Stiefel-Whitney class of the quaternionic projective spaces.* We keep essentially the preceding notations and denote by $\boldsymbol{Q}$ the subgroup of elements of order 2 in $\boldsymbol{T}$. For suitable (1-dimensional) generators u_i of $H^*(B_{\boldsymbol{Q}},\boldsymbol{Z}_2)$, we have [4, § 11]

$$\rho_2{}^*(\boldsymbol{Q},\boldsymbol{T})(x_i)=u_i{}^2 \qquad (i=1,\cdots,q),$$

where here the x_i are elements of $H^2(B_{\boldsymbol{T}},\boldsymbol{Z}_2)$, namely, the reductions mod 2 of the x_i of 15.5. Thus the images of $\rho_2{}^*(\boldsymbol{Q},\boldsymbol{Sp}(q))$ and $\rho_2{}^*(\boldsymbol{Q},\boldsymbol{Sp}(1)\times\boldsymbol{Sp}(q-1))$ are, respectively, $S(u_1{}^4,\cdots,u_q{}^4)$ and $\boldsymbol{Z}_2[u_1{}^4]\otimes S(u_2{}^4,\cdots,u_q{}^4)$, and $H^*(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z}_2)$ may be identified with the quotient of the latter ring by the ideal I generated by the symmetric functions in the $u_i{}^4$ of strictly positive degrees; in particular, $u_1{}^4$ represents the generator $\tilde{u}$ of $H^*(\boldsymbol{P}_{q-1}(\boldsymbol{K}),\boldsymbol{Z}_2)$.

By (5.5), the complementary 2-roots are (u_1-u_i), $(i=2,\cdots,p)$, each counted with multiplicity 4, and therefore, 11.5 gives for the Stiefel-Whitney class of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$:

$$w = \prod_{i=2}^{q} (1 + u_1 - u_i)^4 = \prod_{i=1}^{q} (1 + u_1{}^4 - u_i{}^4) \bmod I$$

which, modulo I, is equal to $(1 + u_1{}^4)^q$, and hence, finally,

$$w(\boldsymbol{P}_{q-1}(\boldsymbol{K})) = (1 + \bar{u})^q,$$

where $\bar{u}$ is the generator of $H^*(\boldsymbol{P}_{q-1}(\boldsymbol{K}), \boldsymbol{Z}_2)$.

The characteristic classes of $\boldsymbol{P}_{q-1}(\boldsymbol{K})$ were calculated in [17] by a different method.

16. Hermitian symmetric spaces.

16.1. We consider here first the homogeneous spaces of the form G/U, where U is the centralizer of a 1-dimensional torus S, has a 1-dimensional center, and G is semi-simple. As was shown in 13.8, such a space admits exactly two invariant complex structures; they are conjugate to each other and equivalent under an automorphism of G.

We may assume that S is defined by $a_1 = \cdots = a_{l-1} = 0$, where $a_1, \cdots, a_l$ are the simple roots with respect to some ordering $\mathcal{S}$. Then (see 13.6, 13.8), the roots of U are the linear combinations of the a_i's with $1 \leqq i \leqq l-1$, and the set Ψ of positive complementary roots is closed and is the root system of one of the two invariant complex structures on G/U, to be denoted by $\mathcal{B}$. Moreover, a root b is in Ψ if and only if, when expressed as a linear combination of the simple roots, the term containing a_l has a strictly positive coefficient. (The space G/U is irreducible hermitian symmetric if and only if G is simple and U is maximal connected. In this case, the coefficients of a_l in the complementary roots are all equal to one and the sum of two elements of Ψ is never a root of G.)

By 14.2, $H^2(G/U, \boldsymbol{Z})$ is infinite cyclic and has a generator g such that $\nu^*(g) = \varpi_l$, where ν is the natural projection of G/T on G/U and ϖ_l is the l-th fundamental weight. If $c_1(G/U)$ denotes the first Chern class of G/U with respect to $\mathcal{B}$, we have then, necessarily, that

$$c_1(G/U) = \lambda(G/U) \cdot g \qquad (\lambda(G/U) \in Z).$$

By 14.7 and 14.8, both g and $c_1(G/U)$ are positive classes, and hence $\lambda(G/U) > 0$. By 10.8, $\nu^*(c_1)$ is equal to the sum of the positive complementary roots, and hence

$$\lambda(G/U) = 2(b, a_l)/(a_l, a_l), \qquad (b = \sum_{a \in \Psi} a).$$

Since the invariant complex structures on G/U are equivalent, $\lambda(G/U)$ does not depend on the choice of the invariant complex structure. Among the spaces considered here are the compact irreducible hermitian symmetric spaces which are divided into six classes, see, e.g., A. Borel, *Bull. Soc. Math. Frances* 80 (1952), 167-182):

I. $\boldsymbol{U}(m+n)/(\boldsymbol{U}(m) \times \boldsymbol{U}(n))$

II. $\boldsymbol{SO}(2n)/\boldsymbol{U}(n)$

III. $\boldsymbol{Sp}(n)/\boldsymbol{U}(n)$

IV. $\boldsymbol{SO}(n+2)/(\boldsymbol{SO}(2) \times \boldsymbol{SO}(n)), \qquad (n > 2)$

V. $\boldsymbol{E}_6/\boldsymbol{Spin}(10) \times \boldsymbol{T}^1$

VI. $\boldsymbol{E}_7/\boldsymbol{E}_6 \times \mathbf{T}^1$.

By the preceding formula, we get for $\lambda(G/U)$ the following values

I. $m+n$, II. $2n-2$, III. $n+1$, IV. n, V. 12, VI. 18.

In the following sections 16.2 to 16.5, we study the non-exceptional types I.-IV. and give formulas for their Chern classes. We also obtain in these cases the values of $\lambda(G/U)$ in a different way. To describe the complex structure on G/U, we choose an ordering having the properties of 13.6. The maximal torus is always chosen in the standard way, i.e., in the cases I, II, III, it is the maximal torus of $\boldsymbol{U}(m+n)$ or $\boldsymbol{U}(n)$ respectively, used in 15.1.

16.2. *The Grassmannian* $\boldsymbol{W}(m,n) = \boldsymbol{U}(m+n)/(\boldsymbol{U}(m) \times \boldsymbol{U}(n))$.

As a system of positive roots of $\boldsymbol{U}(m+n)$, we take

$$\{-x_i + x_j \mid 1 \leqq i < j \leqq m+n\}, \qquad \text{(see 15.1)}.$$

$H^*(\boldsymbol{W}(m,n), \boldsymbol{Z})$ has to be identified with the quotient of

$$S\{x_1, \cdots, x_m\} \otimes S\{x_{m+1}, \cdots, x_{m+n}\} \tag{1}$$

by the ideal I generated by the symmetric power series in $x_1, \cdots, x_{m+n}$ without constant term. The (total) Chern class of $\boldsymbol{W}(m,n)$ is given by

$$c(\boldsymbol{W}(m,n)) = \prod_{\substack{1 \leqq i \leqq m \\ m+1 \leqq j \leqq m+n}} (1 - x_i + x_j) \qquad \operatorname{mod} I.$$

In the tensor product (1), we have

$$\prod_{1 \leqq i \leqq m} (1+x_i)^{-1} = \prod_{m+1 \leqq j \leqq m+n} (1+x_j) \qquad \operatorname{mod} I.$$

The r-th elementary symmetric function in the x_i $(1 \leqq i \leqq m)$ represents an element σ_r of $H^*(\boldsymbol{W}(m,n),\boldsymbol{Z})$. The preceding equation shows that the σ_r $(1 \leqq r \leqq m)$ generate $H^*(\boldsymbol{W}(m,n),\boldsymbol{Z})$. (Recall that we are dealing with graded rings.) The element σ_1 generates the infinite cyclic group $H^2(\boldsymbol{W}(m,n),\boldsymbol{Z})$. Using an indeterminate z, we have

$$(2) \qquad \prod_{m+1 \leqq j \leqq m+n} (z+x_j) = z^{m+n} \prod_{1 \leqq i \leqq m} (z+x_i)^{-1} \qquad \operatorname{mod} I.$$

By replacing in the preceding formula z by $1-x_s$ $(1 \leqq s \leqq m)$, respectively, we obtain m equations; multiplying all of these together yields

$$(3) \qquad c(\boldsymbol{W}(m,n)) = \prod_{i=1}^{m} (1-x_i)^{m+n} \prod_{1 \leqq i \leqq j \leqq m} (1-(x_i-x_j)^2)^{-1} \qquad \operatorname{mod} I.$$

We recall that σ_r is the r-th Chern class of the canonical principal $\boldsymbol{U}(m)$-bundle over $\boldsymbol{W}(m,n)$. Formula (3) expresses $c(\boldsymbol{W}(m,n))$ by the σ_r; for example,

$$c_1(\boldsymbol{W}(m,n)) = -(m+n)\sigma_1,$$

$$c_2(\boldsymbol{W}(m,n)) = (C_2^{m+n} + m - 1)\sigma_1^2 + (n-m)\sigma_2.$$

The formula for the first Chern class gives us the value of $\lambda(\boldsymbol{W}(m,n))$ and shows that $-\sigma_1$ is a positive generator of $H^2(\boldsymbol{W}(m,n),\boldsymbol{Z})$ in the sense of 16.1. For $m=1$, the Grassmannian $\boldsymbol{W}(1,n)$ is the complex projective space $\boldsymbol{P}_n(\boldsymbol{C})$ discussed in 15.1.

16.3. *The space* $\boldsymbol{F}_n = \boldsymbol{SO}(2n)/\boldsymbol{U}(n)$, $(n \geqq 2)$. As a system of positive roots of $\boldsymbol{SO}(2n)$ we take $\{\pm x_i + x_j \mid 1 \leqq i < j \leqq n\}$. We regard the x_i as elements of $H^2(B_T,K_p)$. If $p \neq 2$, then $H^*(\boldsymbol{F}_n,K_p)$ may be identified with the quotient of $S\{x_1,\cdots,x_n\}$ by the ideal I generated by the symmetric power series without constant terms in $x_1^2,\cdots,x_n^2$ and by the element $x_1x_2\cdots x_n$. All power series under consideration have coefficients in K_p. The total Chern class of $\boldsymbol{F}_n$ is given by

$$(4) \qquad c(\boldsymbol{F}_n) = \prod_{1<j} (1+x_i+x_j) \qquad \operatorname{mod} I.$$

The preceding formula expresses the Chern classes of $\boldsymbol{F}_n$ as polynomials in the elementary symmetric functions of the x_i. The coefficients are integral. Let $\sigma_r \in H^{2r}(\boldsymbol{F}_n,\boldsymbol{Z})$ be the r-th Chern class of the canonical $\boldsymbol{U}(n)$-principal bundle over $\boldsymbol{F}_n$. If we reduce σ_r to coefficients K_p $(p \neq 2)$, we get the r-th elementary symmetric function in the x_i (mod I). Since $\boldsymbol{F}_n$ has no torsion, (4) gives a formula for integral cohomology if we replace the r-th elementary symmetric function in the x_i by σ_r. For example, we get

$$c_1(\boldsymbol{F}_n) = (n-1)\sigma_1.$$

σ_1 is not a generator of the infinite cyclic group $H^2(\boldsymbol{F}_n, \boldsymbol{Z})$, but σ_1 equals $2\tilde{g}$, where $\tilde{g}$ is a generator. This is true for $n=2$, since $\boldsymbol{F}_2$ is the complex projective line for which $c_1(\boldsymbol{F}_2)$ is twice a generator. It follows then for all n by induction, using the natural imbedding of $\boldsymbol{F}_n$ in $\boldsymbol{F}_{n+1}$ and the fibre bundle $(\boldsymbol{F}_{n+1}, \boldsymbol{S}_{2n}, \boldsymbol{F}_n)$, see [26, § 41.18]. Thus we have

$$c_1(\boldsymbol{F}_n) = (2n-2)\tilde{g};$$

moreover, $\tilde{g}$ is a positive generator of $H^2(\boldsymbol{F}_n, \boldsymbol{Z})$ and $\lambda(\boldsymbol{F}_n) = 2n-2$ (see 16.1).

16.4. *The space* $\boldsymbol{G}_n = \boldsymbol{Sp}(n)/\boldsymbol{U}(n)$. As a system of positive roots of $\boldsymbol{Sp}(n)$ we take

$$\{\pm x_i + x_j (1 \leqq i < j \leqq n), 2x_i \; (1 \leqq i \leqq n)\}.$$

The integral cohomology ring of $\boldsymbol{G}_n$ has to be identified with the quotient of $S\{x_1, \cdots, x_n\}$ by the ideal I generated by the symmetric power series without constant terms in $x_1^2, \cdots, x_n^2$. The (total) Chern class of $\boldsymbol{G}_n$ is given by

$$c(\boldsymbol{G}_n) = \prod_{1 \leqq i \leqq j \leqq n} (1 + x_i + x_j) \qquad \mathrm{mod}\, I.$$

This formula expresses the Chern classes of $\boldsymbol{G}_n$ by the Chern classes σ_r of the canonical $\boldsymbol{U}(n)$-bundle over $\boldsymbol{G}_n$. The element $x_1 + \cdots + x_n$ represents σ_1, and σ_1 is a generator of the infinite cyclic group $H^2(\boldsymbol{G}_n, \boldsymbol{Z})$; we have

$$c_1(\boldsymbol{G}_n) = (n+1)\sigma_1.$$

Thus σ_1 is a positive generator and $\lambda(\boldsymbol{G}_n) = n+1$ (see (16.1)).

16.5. *The complex quadric* $\boldsymbol{Q}_n = \boldsymbol{SO}(n+2)/(\boldsymbol{SO}(2) \times \boldsymbol{SO}(n))$. We distinguish the two cases (a) n is even and (b) n is odd.

(a) $n+2 = 2k$.

We have the natural imbedding of $\boldsymbol{U}(k)$ in $\boldsymbol{SO}(2k)$ and take for the maximal torus $\boldsymbol{T}$ of $\boldsymbol{SO}(2k)$ the maximal torus of $\boldsymbol{U}(k)$ considered in 15.1. As a system of positive roots of $\boldsymbol{SO}(2k)$, we choose

$$\{x_i \pm x_j \mid 1 \leqq i < j \leqq k\}.$$

The x_i are to be regarded as elements of $H^2(B_T, K_p)$. If $p \neq 2$, then $H^*(\boldsymbol{Q}_n, K_p)$ may be identified with the quotient of the ring V generated by $S\{x_2^2, \cdots, x_k^2\}$ and by the elements $x_2 x_3 \cdots x_k$, x_1 in $K_p\{x_1, x_2, \cdots, x_k\}$ by the ideal I generated by the symmetric power series without constant terms in $x_1^2, \cdots, x_k^2$ and by $x_1 x_2 \cdots x_k$; i.e.,

$$H^*(\boldsymbol{Q}_n, K_p) = V/I.$$

Using an indeterminate z, we have

$$\prod_{i=1}^{k} (z - x_i)(z + x_i) = z^{2k} \qquad \mathrm{mod}\, I. \tag{5}$$

We have also

$$(1 + x_2^2)(1 + x_3^2) \cdots (1 + x_k^2) = (1 + x_1^2)^{-1} \qquad \mathrm{mod}\, I. \tag{6}$$

From (6), we see easily that the elements

$$1, x_1, x_1^2, \cdots, x_1^n, \text{ and } x_2 x_3 \cdots x_k \in V$$

constitute an additive base of $H^*(\boldsymbol{Q}_n, K_p)$. The Chern class of $\boldsymbol{Q}_n$ is given by

$$c(\boldsymbol{Q}_n) = \prod_{j=2}^{k} (1 + x_1 - x_j)(1 + x_1 + x_j) \qquad \mathrm{mod}\, I.$$

Replacing in (5) the indeterminate z by $1 + x_1$, yields

$$c(\boldsymbol{Q}_n) = (1 + x_1)^{n+2}(1 + 2x_1)^{-1} \qquad \mathrm{mod}\, I. \tag{7a}$$

$$n + 1 = 2k. \tag{b}$$

We have the imbedding of $\boldsymbol{U}(k) = \boldsymbol{U}(k) \times 1$ in $\boldsymbol{SO}(2k+1)$ and take for the maximal torus $\boldsymbol{T}$ of $\boldsymbol{SO}(2k+1)$ the maximal torus of $\boldsymbol{U}(k)$ considered in 15.1. As a system of positive roots of $\boldsymbol{SO}(2k+1)$, we choose

$$\{x_i \pm x_j \ (1 \leqq i < j \leqq k) ; x_i \ (1 \leqq i \leqq k)\}.$$

If $p \neq 2$, then $H^*(\boldsymbol{Q}_n, K_p)$ may be identified with the quotient of

$$K_p\{x_1\} \otimes S\{x_2^2, \cdots, x_k^2\}$$

by the ideal I generated by the symmetric power series without constant terms in $x_1^2, \cdots, x_k^2$. As in the case (a), we see that

$$1, x_1, x_1^2, \cdots, x_1^n$$

constitute an additive base of $H^*(\boldsymbol{Q}_n, K_p)$. The Chern class of $\boldsymbol{Q}_n$ is given by

$$c(\boldsymbol{Q}_n) = (1 + x_1) \prod_{j=2}^{k} (1 + x_1 - x_j)(1 + x_1 + x_j), \qquad \mathrm{mod}\, I.$$

The subspace $\mathfrak{u} = \mathfrak{v}_3 + \mathfrak{v}_4 + \mathfrak{v}_6$ is therefore a subalgebra of rank 2 and dimension 6, and hence is isomorphic to the Lie algebra of $\boldsymbol{SO}(4)$, as can also be easily checked directly. Thus the subgroup U of $\boldsymbol{G}_2$ generated by $\mathfrak{u}$ is a compact group locally isomorphic to $\boldsymbol{SO}(4)$, that is, having the product $\boldsymbol{Sp}(1) \times \boldsymbol{Sp}(1)$ as universal covering. It is, in fact, globally isomorphic to $\boldsymbol{SO}(4)$, as can be derived for instance from [7]. In fact, it is proved in [7] that $\boldsymbol{G}_2$ contains exactly one class (relative to inner automorphisms) of subgroups locally isomorphic to $\boldsymbol{SO}(4)$; one of them, say U_1, is the centralizer of a vertex z of order two of a fundamental simplex, and z generates the center of U_1 ([7], Remarque II, p. 220). Looking at the diagram of $\boldsymbol{G}_2$, one sees that the two invariant 3-dimensional subgroups of U_1 are globally isomorphic to $\boldsymbol{Sp}(1)$; since U_1 has a center of order two, it is then isomorphic to $\boldsymbol{SO}(4)$.

17.2. The subgroup $\boldsymbol{Q}$. The relations (1) imply that the linear transformation S_i $(i \in \boldsymbol{Z}_7)$ of $\mathfrak{M}$ which keeps e_{i+1}, e_{i+5}, e_{i+6} fixed and changes the signs of the other e_j's is an automorphism of $\mathfrak{L}$. The seven elements S_i and the identity form a commutative subgroup $\boldsymbol{Q}$ of $\boldsymbol{G}_2$ of type $(2,2,2)$. Moreover, $\boldsymbol{G}_2$ contains no commutative subgroup of type $(2,2,2,2)$ (see A. Borel-J-P. Serre, Comm. Math. Helv. 27 (1953), 128-129 or 17.5).

PROPOSITION. *We keep the previous notations and denote by* x_i *the element of* $\operatorname{Hom}(\boldsymbol{Q}, \boldsymbol{Z}_2)$ *defined by* $x_i(S_j) = \delta_{ij}$ $(1 \leqq i, j \leqq 3)$. *Then* $Q \subset U$, *and the 2-roots of* U *(resp.* $\boldsymbol{G}_2$*) with respect to* $\boldsymbol{Q}$ *are* $x_1 + x_2$, $x_1 + x_3$, $x_2 + x_3$ *(resp. together with* $x_1, x_2, x_3, x_1 + x_2 + x_3$*). Each has multiplicity* 2 *and is the character of* $\boldsymbol{Q}$ *in one of the* $\mathfrak{v}_i$*'s.*

It follows from the definition of U that this group leaves invariant the subspaces $\mathfrak{C}$, $\mathfrak{D}$ of $\mathfrak{M}$ spanned, respectively, by e_3, e_4, e_6 and e_1, e_2, e_5, e_7 and that the restriction to $\mathfrak{D}$ of the standard maximal abelian subgroup $\boldsymbol{Q}'$ of type $(2,2,2)$ of U consists of the diagonal matrices of determinant $+1$. On the other hand, it is readily seen that this is also the restriction of $\boldsymbol{Q}$ to $\mathfrak{D}$; since by (1) an automorphism of $\mathfrak{L}$ leaving e_1, e_2, e_5, e_7 fixed must be the identity, we have $\boldsymbol{Q}' = \boldsymbol{Q}$ and $\boldsymbol{Q} \subset U$. The other assertions follow from the fact that the inner automorphism $\operatorname{Ad} S_i$ defined by S_i is the identity on $\mathfrak{v}_{i+1}$, $\mathfrak{v}_{i+5}$, $\mathfrak{v}_{i+6}$ and is $-\mathrm{Id}$ on the other $\mathfrak{v}_j$'s.

17.3. *The cohomology ring* mod 2 *of* $\boldsymbol{G}_2/\boldsymbol{SO}(4)$. The following facts are proved in [3]: $H^*(B_{SO(4)}, \boldsymbol{Z}_2)$ and $H^*(B_{G_2}, \boldsymbol{Z}_2)$ are rings of polynomials in three variables of degrees 2, 3, 4 and 4, 6, 7 respectively; the homomorphisms $\rho_2^*(\boldsymbol{Q}, \boldsymbol{SO}(4))$ and $\rho_2^*(\boldsymbol{Q}, \boldsymbol{G}_2)$ are injective. The ring $H^*(\boldsymbol{G}_2/\boldsymbol{SO}(4), \boldsymbol{Z}_2)$

is the quotient of $H^*(B_{SO(4)}, \boldsymbol{Z}_2)$ by the ideal generated by the elements of strictly positive degrees in the image of $\rho_2{}^*(\boldsymbol{SO}(4), \boldsymbol{G}_2)$; the Poincaré polynomial mod 2 of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ is

$$P_2(\boldsymbol{G}_2/\boldsymbol{SO}(4), t) = (1-t^4)(1-t^6)(1-t^7)/(1-t^2)(1-t^3)(1-t^4),$$

and hence

$$P_2(\boldsymbol{G}_2/\boldsymbol{SO}(4), t) = 1 + t^2 + t^3 + t^4 + t^5 + t^6 + t^8.$$

PROPOSITION. *We keep the previous notations and denote by* σ_i *the i-th elementary symmetric function in the* x_i*'s. Then the image of* $\rho_2{}^*(\boldsymbol{Q}, U)$ *equals* $\boldsymbol{Z}_2[u_2, u_3, u_4]$ *with* $u_2 = \sigma_2 + \sigma_1{}^2$, $u_3 = \sigma_3 + \sigma_1\sigma_2$, $u_4 = \sigma_1\sigma_3$, *and the image of* $\rho_2{}^*(\boldsymbol{Q}, \boldsymbol{G}_2)$ *equals* $\boldsymbol{Z}_2[g_4, g_6, g_7]$ *with* $g_4 = u_2{}^2 + u_4$, $g_6 = u_3{}^2 + u_2u_4$ *and* $g_7 = u_4u_3$. *Consequently,* $H^*(\boldsymbol{G}_2/\boldsymbol{SO}(4), \boldsymbol{Z}_2)$ *is generated by two elements* u_2, u_3 *of degrees* 2, 3 *with the relations* $u_2{}^3 = u_3{}^2$ *and* $u_3u_2{}^2 = 0$.

We identify U with $\boldsymbol{SO}(4)$ by means of the representation in $\mathfrak{D}$. Let $\boldsymbol{Q}_1$ be the subgroup of diagonal matrices of $\boldsymbol{O}(4)$ and μ the inclusion of $\boldsymbol{Q}$ in $\boldsymbol{Q}_1$. Then, for an obvious choice of a basis (y_1, y_2, y_3, y_4) of $\mathrm{Hom}(\boldsymbol{Q}_1, \boldsymbol{Z}_2)$, the image of $\rho_2{}^*(\boldsymbol{Q}_1, \boldsymbol{O}(4)$ is the ring of symmetric functions in the y_i (cf. [3]), and the homomorphism $\mu'\colon \mathrm{Hom}(\boldsymbol{Q}_1, \boldsymbol{Z}_2) \to \mathrm{Hom}(\boldsymbol{Q}, \boldsymbol{Z}_2)$ induced by μ is given by

$$\mu'(y_i) = x_i \quad (i = 1, 2, 3), \quad \mu'(y_4) = x_1 + x_2 + x_3.$$

Therefore, μ' annihilates $y_1 + y_2 + y_3 + y_4$ and maps the i-th elementary symmetric function in the y_j's onto u_i, for $i = 2, 3, 4$. Since $\rho_2{}^*(Q, \boldsymbol{O}(4))$ and $\rho_2{}^*(Q, \boldsymbol{SO}(4))$ have the same image (see [3]), this proves our first assertion.

The image of $\rho_2{}^*(\boldsymbol{Q}, \boldsymbol{G}_2)$ is a subring of $\boldsymbol{Z}_2[u_2, u_3, u_4]$ generated by elements of degrees 4, 6, 7 and its elements are invariant under the action of the normalizer of $\boldsymbol{Q}$ in $\boldsymbol{G}_2$, operating in the usual way [3]; therefore, in order to prove the second assertion, it suffices to exhibit an automorphism α of $H^*(B_Q, \boldsymbol{Z}_2) = \boldsymbol{Z}_2[x_1, x_2, x_3]$ induced by an inner automorphism of $\boldsymbol{G}_2$, leaving $\boldsymbol{Q}$ invariant, and for which g_i is the only non-zero invariant of degree i $(i = 4, 6, 7)$.

Let S be the linear transformation of $\mathfrak{M}$ which sends $e_1, \cdots, e_7$ onto $e_5, e_7, -e_3, e_4, e_1, -e_6, e_2$ respectively. It follows from (1) that $S \in \boldsymbol{G}_2$. Moreover, it is seen without difficulty that

$$S \cdot S_1 \cdot S = S_1, \quad S \cdot S_2 \cdot S = S_1 \cdot S_3 = S_4, \quad S \cdot S_3 \cdot S = S_1 \cdot S_2 = S_6$$

and, therefore, the automorphism α of $H^*(B_Q, \mathbf{Z}_2)$ induced by Ad S satisfies:

$$(5) \qquad \alpha(x_1) = x_1, \quad \alpha(x_2) = x_1 + x_3, \quad \alpha(x_3) = x_1 + x_2,$$

$$(6) \qquad \alpha(\sigma_1) = \sigma_1, \quad \alpha(\sigma_2) = x_1^2 + x_2x_3, \quad \alpha(\sigma_3) = x_1(x_1^2 + \sigma_2),$$

$$\alpha(u_2) = x_2^2 + x_3^2 + x_2x_3,$$

$$(7) \qquad \alpha(u_3) = x_2x_3(x_2 + x_3),$$

$$\alpha(u_4) = x_1(x_1^2 + \sigma_2)\sigma_1.$$

An element $h \in H^4(B_U, \mathbf{Z}_2)$ may be written in the form $h = a \cdot u_4 + b \cdot u_2^2$ $(a, b \in \mathbf{Z}_2)$, and hence

$$\alpha(h) = ax_1(x_1^2 + \sigma_2)\sigma_1 + bx_2^2x_3^2 + b(x_2^4 + x_3^4).$$

The coefficients of x_1^4 in h and $\alpha(h)$ are b and a respectively; therefore, if $h = \alpha(h)$ with $h \neq 0$ we must have $a = b = 1$ and $h = g_4$. That g_4 is in fact invariant under α can be checked directly, but this is not necessary since we know a priori that $H^4(B_{G_2}, \mathbf{Z}_2)$ has dimension one.

The proofs of the invariance of g_6, g_7 under α are quite analogous: an element of degree six may be written

$$h = au_2^3 + bu_3^2 + cu_2g_4 \qquad (a, b, c \in \mathbf{Z}_2).$$

Using (7), one sees that the coefficients of x_1^6 in h and $\alpha(h)$ are $a + c$ and zero respectively, while those of $x_1^4 \cdot x_2^2$ are $a + b + c$ and c. Thus $\alpha(h) = h$ and $h \neq 0$ imply $a = b = c = 1$ and $h = g_6$. Finally, starting with a general element

$$h = u_3(au_2^2 + bg_4) \qquad (a, b \in \mathbf{Z}_2)$$

of degree seven, we see by looking at the coefficients of $x_1^6 \cdot x_2$ that $h = \alpha(h)$ and $h \neq 0$ imply $a = b = 1$, that is $h = g_7$.

The last assertion follows then from the results recalled at the beginning of 17.3.

17.4. PROPOSITION. *The Stiefel-Whitney classes of $\mathbf{G}_2/\mathbf{SO}(4)$ are non-zero only in the dimensions* 0, 4, 6, 8.

By 11.5 and 17.2, the image under $\rho_2^*(\mathbf{Q}, U)$ of the total Stiefel-Whitney class of the bundle along the fibres of $(B_U, B_{G_2}, \mathbf{G}/U)$ is

$$w' = (1 + \sigma_1)^2 \cdot \prod_1^3 (1 + x_i)^2;$$

therefore

$$w' = (1 + \sigma_1^2 + \sigma_2^2 + \sigma_3^2)(1 + \sigma_1^2) = 1 + u_2^2 + u_3^2 + u_4^2;$$

and 17.4 follows now from 17.3.

17.5. *Remarks.* 1) The 2-roots of $\boldsymbol{G}_2$ have been computed with respect to a particular subgroup of type (2, 2, 2). In fact, these subgroups are conjugate by inner automorphisms, and these 2-roots are therefore invariants of $\boldsymbol{G}_2$. To see this, one uses the fact that given three orthonormal purely imaginary Cayley numbers u, v, w with w also orthogonal to $u \cdot v$, there exists exactly one automorphism of $\mathfrak{K}$ which maps e_1, e_2, e_3 onto u, v, w, respectively (see N. Jacobson, *Duke Math. Jour.* 5 (1939), 776-783). This implies easily that any commutative subgroup of type (2, 2, 2) of $\boldsymbol{G}_2$ can be put in the diagonal form by means of an automorphism of $\boldsymbol{G}_2$. Moreover, one deduces from (1) that $\boldsymbol{Q}$ contains all diagonal matrices of $\boldsymbol{G}_2$; hence, $\boldsymbol{G}_2$ does not contain commutative subgroups of type (2, 2, 2, 2).

(2) It follows a posteriori from the proof of 17.3 that $\rho_{20}(\boldsymbol{Q}, \boldsymbol{G}_2)$ maps $H^*(B_{G_2}, \boldsymbol{Z}_2)$ isomorphically onto the ring of invariants of the normalizer of $\boldsymbol{Q}$ in $\boldsymbol{G}_2$. Thus, the analogy between the role of $\boldsymbol{Q}$ in cohomology mod 2 and that of a maximal torus in real cohomology, which is the basis of [3], is also very complete for $\boldsymbol{G}_2$.

18. Some manifolds with Poincaré polynomial $1 + t^4 + t^8$.

18.1. The quaternionic plane $\boldsymbol{P}_2(\boldsymbol{K})$ is an 8-dimensional manifold with real Poincaré polynomial $1 + t^4 + t^8$. We know (15.5) that the (integral) Pontrjagin class of $\boldsymbol{P}_2(\boldsymbol{K})$ is given by

$$p = (1 + u)^6(1 + 4u)^{-1}.$$

Thus $p_1 = 2u$ and $p_2 = 7u^2$. The Pontrjagin numbers of $\boldsymbol{P}_2(\boldsymbol{K})$ are

$$p_1^2[\boldsymbol{P}_2(\boldsymbol{K})] = 4 \quad \text{and} \quad p_2[\boldsymbol{P}_2(\boldsymbol{K})] = 7.$$

Here we use the orientation defined by $u^2[\boldsymbol{P}_2(\boldsymbol{K})] = 1$.

18.2. The manifolds $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ (see § 17) and $\tilde{\boldsymbol{Q}}_4$ (see 16.6) have the real Poincaré polynomial $1 + t^4 + t^8$. Their Pontrjagin numbers are (for suitable orientations) the same as those of the quaternionic plane. For $\tilde{\boldsymbol{Q}}_4$, this was proved already in 16.6. In the next section, it will be shown for $\boldsymbol{G}_2/\boldsymbol{SO}(4)$. We do not know whether all differentiable manifolds with real Poincaré polynomial $1+t^4+t^8$ have the same Pontrjagin numbers. By the index theorem ([19], p. 85), we know for such a manifold X that (for suitable orientation)

$$(7p_2-p_1^2)[X]=45, \tag{1}$$

and therefore, it is sufficient to calculate one Pontrjagin number. But, as an example, we shall make the computations without the use of the index theorem in the case of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$.

Remark. Milnor has constructed an 8-dimensional combinatorial manifold with real Poincaré polynomial $1+t^4+t^8$ whose Pontrjagin numbers (in the sense of Thom) satisfy (1), but are rational, non-integral numbers. This manifold of Milnor does not admit a differentiable structure compatible with its combinatorial structure.

18.3. By the Hirsch formula, the manifold $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ has the real Poincaré polynomial $(1-t^4)(1-t^{12})(1-t^4)^{-1}(1-t^4)^{-1}=1+t^4+t^8$. We calculate the Pontrjagin class of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ by the schema used in 15.5. All cohomology groups are taken with real coefficients.

Roots of $\boldsymbol{G}_2$:

$$\pm x_1,\ \pm x_2,\ \pm(x_1-x_2),\ \pm(x_1-2x_2),\ \pm(x_1-3x_2),\ \pm(2x_1-3x_2)$$

with respect to a convenient base $x_1, x_2 \in H^2(\boldsymbol{G}_2/T)$ for a maximal torus T of $\boldsymbol{G}_2$.

Following de Siebenthal [25a] we take $\phi_1=x_2$ and $\phi_2=x_1-3x_2$ as simple roots of $\boldsymbol{G}_2$. The dominant root is then $3\phi_1+2\phi_2=2x_1-3x_2$. By [7, p. 218], we know that there is an imbedding of $\boldsymbol{SO}(4)$ in $\boldsymbol{G}_2$ for which $\pm\phi_1$ and $\pm(3\phi_1+2\phi_2)$ are the roots of $\boldsymbol{SO}(4)$.

Complementary roots: $\pm x_1,\ \pm(x_1-x_2),\ \pm(x_1-2x_2),\ \pm(x_1-3x_2)$.

We put $y_1=2x_1-3x_2$ and $y_2=x_2$.

Invariants of the Weyl group of $\boldsymbol{G}_2$: Since $H^*(B_{\boldsymbol{G}_2})$ is the polynomial ring over $\boldsymbol{R}$ in two indeterminates of degrees 4 and 12, we have only one invariant in dimension 4. Since the dimension of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ equals 8, this is the only invariant we need. An invariant of dimension 4 is always given by the sum of the squares of all roots, which, up to a factor, is, in our case,

$$4(x_1^2-3x_1x_2+3x_2^2)=(y_1^2+3y_2^2).$$

It is convenient to express the complementary roots as linear combinations of y_1, y_2. This gives

$$\begin{aligned} x_1 &= \tfrac{1}{2}(y_1 + 3y_2), \\ x_1 - x_2 &= \tfrac{1}{2}(y_1 + y_2), \\ x_1 - 2x_2 &= \tfrac{1}{2}(y_1 - y_2), \\ x_1 - 3x_2 &= \tfrac{1}{2}(y_1 - 3y_2). \end{aligned}$$

Euler class W *of* $\boldsymbol{G}_2/\boldsymbol{SO}(4)$:

$$\pm 16W = (y_1^2 - y_2^2)(y_1^2 - 9y_2^2) = 4y_2^2 \cdot 12y_2^2,$$
$$\pm W = 3y_2^4,$$

the computations being made modulo the invariants. Since the Euler number of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ equals 3, we get

$$y_2^4[\boldsymbol{G}_2/\boldsymbol{SO}(4)] = 1 \tag{2}$$

after choosing the orientation of $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ conveniently.

The Pontrjagin class p *of* $\boldsymbol{G}_2/\boldsymbol{SO}(4)$:

$$\begin{aligned} 1 + 4p_1 + 16p_2 &= (1 + (y_1 + 3y_2)^2)(1 + (y_1 - 3y_2)^2)(1 + (y_1 - y_2)^2)(1 + (y_1 + y_2)^2) \\ &= (1 + 2(y_1^2 + 9y_2^2) + (y_1^2 - 9y_2^2)^2)(1 + 2(y_1^2 + y_2^2) + (y_1^2 - y_2^2)^2) \\ &= (1 + 12y_2^2 + 144y_2^4)(1 - 4y_2^2 + 16y_2^4). \end{aligned}$$

$$1 + p_1 + p_2 = (1 + 3y_2^2 + 9y_2^4)(1 - y_2^2 + y_2^4),$$
$$p_1 = 2y_2^2, \qquad p_2 = 7y_2^4.$$

(All calculations modulo the invariants.)

By (2), we get for the Pontrjagin numbers (with respect to the orientation defined by (2))

$$p_1^2[\boldsymbol{G}_2/\boldsymbol{SO}(4)] = 4, \qquad p_2[\boldsymbol{G}_2/\boldsymbol{SO}(4)] = 7.$$

19. The Cayley plane.

19.1. The center of the simply connected representative of the local structure $\boldsymbol{F}_4$ consists only of the unit element, as is well known. The structure $\boldsymbol{F}_4$ has, therefore, one and only one representative which we also denote by $\boldsymbol{F}_4$. According to [7], the group $\boldsymbol{F}_4$ contains exactly one class (relative to inner automorphisms) of subgroups with local structure $\boldsymbol{B}_4$. They are, in fact, globally isomorphic to $\boldsymbol{Spin}(9)$. The homogeneous space $\boldsymbol{F}_4/\boldsymbol{Spin}(9)$ has dimension 16 and may be identified with the Cayley plane W, the projective plane over the Cayley-numbers. The Cayley plane $\boldsymbol{W}$, considered as the homogeneous space $\boldsymbol{F}_4/\boldsymbol{Spin}(9)$, was studied, for instance, in [1], see also [2], § 29 and Freudenthal, loc. cit.,[8] § 17. The integral cohomology of $\boldsymbol{W}$ is given by

$$H^0 = H^8 = H^{16} = Z, \qquad H^i = 0 \text{ otherwise.}$$

19.2. Let $\boldsymbol{T}$ be the standard maximal torus of $\boldsymbol{SO}(9)$ with the base $x_1, x_2, x_3, x_4 \in H^1(\boldsymbol{T}, \boldsymbol{Z})$ (see 16.5(b)). Then the roots of $\boldsymbol{SO}(9)$ are

$$\pm x_i \pm x_j \ (1 \leqq i < j \leqq 4)\,; \quad \pm x_1, \pm x_2, \pm x_3, \pm x_4. \tag{1}$$

We have the projection

$$\pi\colon \boldsymbol{Spin}(9) \to \boldsymbol{SO}(9).$$

$\pi^{-1}(\boldsymbol{T}) = \boldsymbol{T}'$ is a maximal torus of $\boldsymbol{Spin}(9)$. The restriction of π to $\boldsymbol{T}'$ induces an isomorphism of $H^1(\boldsymbol{T}, \boldsymbol{R})$ onto $H^1(\boldsymbol{T}', \boldsymbol{R})$. Thus x_1, x_2, x_3, x_4 may be regarded as elements of $H^1(\boldsymbol{T}', \boldsymbol{R})$. They constitute a base of $H^1(\boldsymbol{T}', \boldsymbol{R})$. By [7, Théorème 4], we can choose an embedding of $\boldsymbol{Spin}(9)$ in $\boldsymbol{F}_4$ such that the roots of $\boldsymbol{F}_4$ with respect to $\boldsymbol{T}'$ (considered as elements of $H^1(\boldsymbol{T}', \boldsymbol{R})$) are those given in (1) together with the following (see, e.g., [25a]):

$$\tfrac{1}{2}(\pm x_1 \pm x_2 \pm x_3 \pm x_4), \tag{2}$$

which are the roots of $\boldsymbol{F}_4$ complementary to $\boldsymbol{Spin}(9)$. We now regard x_1, x_2, x_3, x_4 as elements of $H^2(B_{\boldsymbol{T}'}, \boldsymbol{R})$. We introduce the elementary symmetric functions $a_1, \cdots, a_4$ in the x_i^2

$$1 + a_1 + a_2 + a_3 + a_4 = \prod_{i=1}^{4} (1 + x_i^2). \tag{3}$$

The polynomials

$$a_1, \; -6a_3 + a_1 a_2, \; 12a_4 + a_2^2 - \tfrac{1}{2} a_1^2 a_2 \tag{4}$$

are invariants of the Weyl group of $\boldsymbol{F}_4$.

Proof. Since the a_i are invariants of the Weyl group of $\boldsymbol{Spin}(9)$, it suffices to check that the polynomials (4) are invariant under the reflection to the plane

$$x_1 + x_2 + x_3 + x_4 = 0,$$

with respect to the usual Euclidean metric.

19.3. The calculation of the Pontrjagin class of $\boldsymbol{W}$ goes in the same way as for $\boldsymbol{G}_2/\boldsymbol{SO}(4)$ (see § 18). We indicate briefly the various steps of the computation. We put

$$r_i = \tfrac{1}{2}(x_1 \pm x_2 \pm x_3 \pm x_4), \qquad (i = 1, 2, \cdots, 8).$$

For the Pontrjagin class with real coefficients, we get, modulo the invariants (4),

$$p(\boldsymbol{W}) = \prod_{i=1}^{8} (1 + r_i^2) = 1 - a_2 - 13a_4, \text{ i.e.,}$$

$$p_1 = p_3 = 0, \quad p_2 = -a_2, \quad p_4 = -13a_4, \tag{5}$$

$$p_2^2 = a_2^2 = -12a_4. \tag{6}$$

Let u be a generator of the infinite cyclic group $H^8(\boldsymbol{W}, \boldsymbol{Z})$. Then the Euler class of $\boldsymbol{W}$ equals $\pm 3u^2$. On the other hand, we have, after reducing to real coefficients and modulo the invariants (4),

$$\pm 3u^2 = \prod_{i=1}^{8} r_i = - a_4 = a_2^2/12.$$

The preceding equation and (6) yield, since p_2 is a real multiple of u,

$$p_2^2 = +36u^2, \qquad p_2 = \pm 6u, \tag{7}$$

$$p_4 = 39u^2. \tag{8}$$

Since $\boldsymbol{W}$ is without torsion, we conclude that (7) and (8) are also true in integral cohomology. We choose the generator u such that $p_2 = 6u$.

19.4. THEOREM. *There exists a generator u of the infinite cyclic group $H^8(\boldsymbol{W}, \boldsymbol{Z})$ such that the integral Pontrjagin classes of W are given by*

$$p_2(\boldsymbol{W}) = 6u, \qquad p_4(\boldsymbol{W}) = 39u^2.$$

Choosing that orientation of $\boldsymbol{W}$ which is defined by u^2, the non-vanishing Pontrjagin numbers of $\boldsymbol{W}$ are

$$p_2^2[\boldsymbol{W}] = 36, \qquad p_4[\boldsymbol{W}] = 39. \tag{9}$$

19.5. The manifold $\boldsymbol{W}$, oriented as in 19.4, has the index $\tau(\boldsymbol{W}) = 1$. By the index theorem ([19], Satz 8.2.2), we have

$$(381p_4 - 19p_2^2)[\boldsymbol{W}] = 3^4 \cdot 5^2 \cdot 7. \tag{10}$$

We shall see later in this paper by some general arguments that the A-genus ([19], 1.6) of $\boldsymbol{W}$ vanishes. This, together with (10), gives a system of two linear equations for the Pontrjagin numbers from which (9) can also be obtained.

19.6. From Theorem 19.4, we can easily draw the following consequences.

(a) Let $\mathcal{P}_5^1$ be the Steenrod reduced power

$$\mathcal{P}_5^1 \colon H^k(X, \boldsymbol{Z}_5) \rightarrow H^{k+8}(X, \boldsymbol{Z}_5).$$

For the generator u of 19.4 we have, by [15] (coefficients reduced to $\boldsymbol{Z}_5$),

$$\mathcal{P}_5^1 u = \tfrac{1}{9}(7p_2 - p_1^2)u = -2p_2 u = -2u^2. \tag{11}$$

(11) implies that, for each homeomorphism ϕ of $\boldsymbol{W}$ onto $\boldsymbol{W}$, we have $\phi^* u = u$.

(b) The manifold $\boldsymbol{W}$ with its usual differentiable structure does not admit an almost complex structure.

Proof.

$$c^2 = (1 + c_4 + c_8)^2 = 1 + 6u + 39u^2$$

would imply

$$c_8 = 15u^2,$$

but, for an almost complex structure, we would have

$$c_8 = \pm 3u^2.$$

(c) The (total) Stiefel-Whitney class w of $\boldsymbol{W}$ is

$$w = 1 + u + u^2 \text{ (coefficients reduced to } \boldsymbol{Z}_2).$$

Proof. We have (coefficients reduced to $\boldsymbol{Z}_2$), see 9.2, 9.3 and Appendix II,

$$w_8^2 = p_4, \qquad w_{16} = 3u^2 \text{ (Euler class).}$$

INSTITUTE FOR ADVANCED STUDY,
UNIVERSITY OF BONN, GERMANY.

REFERENCES.

[1] A. Borel, "Le plan projectif des octaves et les sphères comme espaces homogènes," *Comptes Rendus*, vol. 230 (1950), pp. 1378-1380.

[2] ———, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[3] ———, "La cohomologie mod 2 de certains espaces homogènes," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 165-191.

[4] ———, "Sur l'homologie et la cohomologie des groupes de Lie compacts connexes," *American Journal of Mathematics*, vol. 76 (1954), pp. 273-342.

[5] ———, "Kählerian coset spaces of semi-simple Lie groups," *Proceedings of the National Academy of Sciences*, vol. 40 (1954), pp. 1147-1151.

[6] ——— and J-P. Serre, "Groupes de Lie et puissances réduites de Steenrod," *American Journal of Mathematics*, vol. 75 (1953), pp. 409-448.

[7] ——— and J. de Siebenthal, "Sur les sous-groupes fermés de rang maximum des groupes de Lie compacts connexes," *Commentarii Mathematici Helvetici*, vol. 23 (1949), pp. 200-221.

[7a] ——— and A. Weil, "Représentations linéaires et espaces homogènes kähleriens des groupes de Lie compacts," Séminaire Bourbaki, May 1954 (Exposé by J-P. Serre).

[7b] R. Bott, "Homogeneous vector bundles," *Annals of Mathematics*, vol. 66 (1957), pp. 203-248.

[8] E. Cartan, "La géométrie des groupes simples," *Annali di Matematica*, vol. 4 (1927), pp. 209-256, vol. 5 (1928), pp. 253-260.

[9] S. S. Chern, "Characteristic classes of hermitian manifolds," *Annals of Mathematics*, vol. 47 (1946), pp. 85-121.

[10] ———, "Topics in differential geometry," Notes, Institute for Advanced Study, Princeton 1951.

[11] ———, "On the characteristic classes of complex sphere bundles and algebraic varieties," *American Journal of Mathemctics*, vol. 75 (1953), pp. 565-597.

[12] S. S. Chern, F. Hirzebruch, J-P. Serre, "On the index of a fibred manifold," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 587-596.

[13] E. B. Dynkin, "The structure of semi-simple Lie algebras," Uspehi Matematiceskih Nauk (N. S.), vol. 2 (1947), pp. 59-127, translated in *American Mathematical Society Translations* 17, 1950.

[14] A. Frölicher, "Zur Differentialgeometrie der komplexen Strukturen," *Mathematische Annalen*, vol. 129 (1955), pp. 50-95.

[15] F. Hirzebruch, "On Steenrod's reduced powers, the index of inertia, and the Todd genus," *Proceedings of the Academy of Sciences of the U. S. A.*, vol. 39 (1953), pp. 951-956.

[16] ———, "Todd arithmetic genus for almost complex manifolds," "On Steenrod's reduced powers in oriented manifolds," "The index of an oriented manifold and the Todd genus of an almost complex manifold," Notes, Princeton University, 1953.

[17] ———, "Über die quaternionalen projektiven Räume," *Bayerische Akademie der Wissenschaften* (1954), pp. 301-312.

[18] ———, "Some problems on differentiable and complex manifolds," *Annals of Mathematics*, vol. 60 (1954), pp. 213-236.

[19] ———, "Neue topologische Methoden in der algebraischen Geometrie," *Ergebnisse der Mathematik und ihrer Grenzgebiete* (N. F.) 9, Berlin, 1956.

[20] W. V. D. Hodge, "The characteristic classes on algebraic varieties," *Proceedings of the London Mathematical Society*, (3), vol. 1 (1951), pp. 138-151.

[21] H. Hopf und H. Samelson, "Ein Satz über die Wirkungsräume geschlossener Liescher Gruppen," *Commentarii Mathematici Helvetici*, vol. 13 (1940-41), pp. 240-251.

[22] K. Kodaira, "On a differential-geometric method in the theory of analytic stacks," *Proceedings of the National Academy of Sciences of the U. S. A.*, vol. 39 (1953), pp. 1268-1273.

[23] "Groupes et algèbres de Lie," Séminaire S. Lie, Notes, Paris, 1954.

[24] W. Rohlin, "New results in the theory of four-dimensional manifolds" (in Russian), Doklady Akademii Nauk S. S. S. R. 84 (1952), pp. 221-224.

[25] J-P. Serre, "Groupes d'homotopie et classes de groupes abéliens," *Annals of Mathematics*, vol. 58 (1953), pp. 258-294.

[25a] J. de Siebenthal, "Sur les sous-groupes fermés connexes des groupes de Lie clos," *Commentarii Mathematici Helvetici*, vol. 25 (1951), pp. 210-256.

[26] N. Steenrod, "Topology of fibre bundles," *Princeton Mathematical Series*, no. 14.

[27] E. Stiefel, "Ueber eine Beziehung zwischen geschlossenen Lie'schen Gruppen und . . .", *Commentarii Mathematici Helvetici*, vol. 14 (1941-42), pp. 350-380.

[28] ———, "Kristallographische Bestimmung der Charaktere der geschlossenen Lie'schen Gruppen," *Commentarii Mathematici Helvetici*, vol. 14 (1944-45), pp. 165-200.

[29] R. Thom, "Quelques propriétés globales des variétés différentiables," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 17-86.

[30] H. Toda, "Quelques tables des groupes d'homotopie des groupes de Lie," *Comptes Rendus*, vol. 241 (1955), pp. 922-923.

[31] H. C. Wang, "Closed manifolds with homogeneous complex structure," *American Journal of Mathematics*, vol. 76 (1954), pp. 1-32.

[32] H. Weyl, "Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen I, II, III," *Mathematische Zeitschrift*, vol. 23 (1925), pp. 271-309, vol. 24 (1926), pp. 328-395.

THE CRITERION FOR UNIT MULTIPLICITY AND A GENERALIZATION OF HENSEL'S LEMMA.*[1]

By Wei-Liang Chow.

To Artin on his 60th birthday

The well-known criterion for unit multiplicity in algebraic geometry states that if two cycles $\mathfrak{X}^r$ and $\mathfrak{Y}^s$ in a variety V^n $(n=r+s)$ are transversal to each other at a simple point α in V, then $\mathfrak{X}$ and $\mathfrak{Y}$ intersect properly at α with the multiplicity 1. This is the version of the criterion as formulated in Weil's *Foundations of Algebraic Geometry*,[2] whereby we have restricted ourselves for simplicity to the case $r+s=n$. It is possible to give this criterion another formulation which is somewhat more elementary in the sense that it involves the multiplicity of a specialization rather than that of an intersection. It can be stated as follows: If two cycles $\mathfrak{X}^r$ and $\mathfrak{Y}^s$ are specializations of two subvarieties $\mathfrak{X}'$ and $\mathfrak{Y}'$ respectively in a variety V^n $(n=r+s)$ over a field of definition k for V, if $\mathfrak{X}'\cap\mathfrak{Y}'$ consists of a finite set of (distinct) points $a^{(i)}$, and if $\mathfrak{X}$ and $\mathfrak{Y}$ are transversal to each other at a simple point α in V, then the point α occurs exactly once in every specialization of the set $a^{(i)}$ over the specialization $(\mathfrak{X}',\mathfrak{Y}')\rightarrow(\mathfrak{X},\mathfrak{Y})$ over k. This version of the criterion for unit multiplicity appeared in the earlier intersection theory of van der Waerden,[3] and played an essential role there in the development of the concept of the intersection-multiplicity itself. However, if one examines very closely the treatment of van der Waerden, one observes that only a part of this criterion, namely the assertion that the specialization-multiplicity is *at most* one, was given a simple proof before the introduction of the concept of the intersection-multiplicity, while the other part, which asserts that this specialization-multiplicity is *at least* one, was proved only later after the concept of the intersection-multiplicity had

---

* Received January 17, 1958.

[1] This work was partially supported by a research grant of the National Science Foundation.

[2] See Chapter VI, Theorem 6.

[3] B. L. van der Waerden, "Zur algebraischen Geometrie V. Ein Kriterium fuer die Einfachheit von Schnittpunkten," *Math. Annalen*, 110, 128-133, 1934.

already been introduced.[4] In fact, this second part concerning the positivity of this particular specialization-multiplicity was proved by van der Waerden in a rather complicated and indirect way, at first only for cycles in a projective space and later carried over to the general case. As we have recently developed a new theory of intersection which preserves the basic ideas of the original theory of van der Waerden, although in an extensively generalized form, we become naturally interested in finding a proof of the criterion for unit multiplicity which is completely free from any use of the notion of the intersection-multiplicity. It turns out that we are able not only to find a simple proof of this nature, but also at the same time, by virtue of the abstract local form in which we have recast this criterion itself, to obtain a more precise result which contains as a special case a certain generalization of the Hensel's Lemma conjectured by Weil some years ago. Although the subject forms an integral part of our intersection theory, which will be published elsewhere at a later date, we feel that this connection with the Hensel's Lemma justifies its separate publication here as a short note. In keeping with the foundational nature of the subject, we shall make our treatment as elementary as posible, using only a few elementary properties in the theory of local rings. Finally, we shall show in the last section that this connection with Hensel's Lemma can be extended to a more general result in the intersection-theory, namely the invariance of intersection-multiplicity under specialization; it turns out that this invariance can be easily deduced from the Associativity Formula, as generalized in a recent paper[5] of Nagata. Here we shall of course need the more sophisticated results in the theory of local rings.

1. Let K be a field, and let v be a real discrete valuation of K; let K_v be the valuation ring of v in K, let π be a generator of its maximal prime ideal, and let $\bar{K}$ be the residue field of K_v modulo the maximal prime ideal. We denote by S^m and $\bar{S}^m$ the projective spaces over the fields K and $\bar{K}$ respectively, and we shall be interested in the relation between the varieties and cycles contained in them. Let α be a rational point over $\bar{K}$ in $\bar{S}^m$. We choose an affine coordinate system in S^m so that in the corresponding affine coordinate system in $\bar{S}^m$ the point α is at the origin; we introduce

---

[4] The first part was proved in the paper cited above; the second part is contained implicitly in B. L. van der Waerden, "Zur algebraischen Geometrie, XIV. Schnittpunktszahlen von algebraischen Mannigfaltigkeiten," *Math. Annalen*, 115, 619-642, 1938, see § 4.

[5] M. Nagata, "The Theory of Multiplicity in General Local Rings," *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo-Nikko 1955, pp. 191-226.

the indeterminates $X_1, \cdots, X_m$ corresponding to the affine coordinates so that we have $\alpha = (0, \cdots, 0)$ and consider the ring $K[X] = K[X_1, \cdots, X_m]$ as well as the rings $K_v[X] = K_v[X_1, \cdots, X_m]$ and $\bar{K}[X] = \bar{K}[X_1, \cdots, X_m]$. The canonical homomorphism E of K_v onto $\bar{K}$ can be extended to a homomorphism of the polynomial ring $K_v[X]$ onto the polynomial ring $\bar{K}[X]$, and for any $f(X)$ in $K_v[X]$ we shall denote its image under E in $\bar{K}[X]$ by $\bar{f}(X)$. Let $\mathfrak{Q}(S/\alpha)$ be the set of all quotients $f(X)/g(X)$ of two elements $f(X)$ and $g(X)$ in $K_v[X]$ such that $\bar{g}(\alpha) \neq 0$; it is easily seen that $\mathfrak{Q}(S/\alpha)$ is a local ring and that its maximal prime ideal $p(S/\alpha)$ is generated by the $m + 1$ elements $\pi, X_1, \cdots, X_m$. Similarly, let $\mathfrak{Q}(\bar{S}/\alpha)$ be the set of all quotients $\phi(X)/\theta(X)$ of two elements $\phi(X)$ and $\theta(X)$ in $\bar{K}[X]$ such that $\theta(\alpha) \neq 0$; it is well known that $\mathfrak{Q}(\bar{S}/\alpha)$ is a regular local ring of dimension m and that it maximal prime ideal $p(\bar{S}/\alpha)$ is generated by the m elements $X_1, \cdots, X_m$. It is easily seen that the homomorphism E of $K_v[X]$ onto $\bar{K}[X]$ can be extended to a homomorphism of $\mathfrak{Q}(S/\alpha)$ onto $\mathfrak{Q}(\bar{S}/\alpha)$ and that the kernel of the so extended homomorphism E is the ideal in $\mathfrak{Q}(S/\alpha)$ generated by the element π. This shows, in particular, that $\mathfrak{Q}(S/\alpha)$ has a dimension at least $m + 1$, and since $p(S/\alpha)$ is generated by the $m + 1$ elements $\pi, X_1, \cdots, X_m$, it follows that $\mathfrak{Q}(S/\alpha)$ is a regular local ring of dimension $m + 1$.

Let $\mathfrak{X}^r$ be a positive cycle in S^m, rational over K, and let $F(U) = F({}_0U, {}_1U, \cdots, {}_rU)$ be the associated form of $\mathfrak{X}$, where each ${}_iU$ is a system of $m + 1$ indeterminates; by a proper choice of the proportionality factor, we can obtain that the coefficients in $F(U)$ are all in K_v, but not all in the maximal prime ideal, and we observe that in this way the coefficients in $F(U)$ are uniquely determined up to a common factor which is a unit in K_v. If we denote by $\bar{F}(U)$ the form obtained from $F(U)$ by replacing every coefficient by its image in $\bar{K}$, then $\bar{F}(U)$ is the associated form of a positive r-cycle $\bar{\mathfrak{X}}$ in $\bar{S}^m$; since the form $\bar{F}(U)$ is uniquely determined up to a factor in $\bar{K}$ by the form $F(U)$, the cycle $\bar{\mathfrak{X}}$ is uniquely determined by the cycle $\mathfrak{X}$. We shall call the cycle $\bar{\mathfrak{X}}$ the *specialization of the cycle $\mathfrak{X}$ over the valuation v.* We shall now express this situation in terms of local ideals at a given point in $\bar{\mathfrak{X}}$. Let α be a point in $\bar{\mathfrak{X}}$ (i.e., a point in the support of $\bar{\mathfrak{X}}$), rational over $\bar{K}$, and assume that an affine coordinate system in S^m has been chosen as indicated above. Let $\mathfrak{P}$ be the ideal in $K[X]$ associated with the support of the positive cycle $\mathfrak{X}$, i.e., $\mathfrak{P}$ consists of all polynomials in $K[X]$ which vanish at every point in the support of $\mathfrak{X}$; we set $\mathfrak{P}_v = K_v[X] \cap \mathfrak{P}$ and $\mathfrak{P}_\alpha = \mathfrak{Q}(S/\alpha)\mathfrak{P}_v$. The fact that $\mathfrak{X}$ has the dimension r can be expressed by the property that every minimal prime divisor of $\mathfrak{P}$ has the rank $m - r$;

we recall that the rank of a prime ideal is defined as the maximum length of a descending chain of prime ideals starting with, but not including, the given ideal itself, and the rank of any ideal is defined as the minimum of the ranks of its minimal prime divisors. Since every element in $\mathfrak{P}$ can be made into an element in $\mathfrak{P}_v$ by multiplying with a suitable power of π, it follows that every minimal prime divisor of $\mathfrak{P}_v$ must have the same rank $m-r$; since $\mathfrak{X}$ contains the point α, the ideal $p(S/\alpha)$ contains $\mathfrak{P}_\alpha$, and it follows then from well-known properties of quotient rings that every minimal prime divisor of $\mathfrak{P}_\alpha$ must have the same rank $m-r$ as $\mathfrak{P}_v$. Let $\bar{\mathfrak{P}}_v$ be the image ideal of $\mathfrak{P}_v$ under the homomorphism E; then $\bar{\mathfrak{P}}_v$ is contained in the ideal associated with the support of $\bar{\mathfrak{X}}$, and hence every minimal prime divisor of $\bar{\mathfrak{P}}_v$ must have a rank at most $m-r$. If we denote by $\bar{\mathfrak{P}}_\alpha$ the image ideal of $\mathfrak{P}_\alpha$ under the homomorphism E, then it is easily seen that $\bar{\mathfrak{P}}_\alpha = \mathfrak{Q}(\bar{S}/\alpha)\bar{\mathfrak{P}}_v$; hence $\bar{\mathfrak{P}}_\alpha$ must have a rank at most $m-r$.

We shall say that the positive cycle $\bar{\mathfrak{X}}$ is *simple* at the point α if exactly one component variety $\bar{\mathfrak{X}}_\alpha$ in $\bar{\mathfrak{X}}$, with the coefficient 1, contains the point α, and if this component is simple at α.

LEMMA 1. *If the cycle $\bar{\mathfrak{X}}$ is simple at the point α, then $\bar{\mathfrak{P}}_\alpha$ has a basis consisting of $m-r$ elements which can be extended to a minimal basis for $p(\bar{S}/\alpha)$; and when such is the case, then $\bar{\mathfrak{P}}_\alpha$ is the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha)$ associated with the variety $\bar{\mathfrak{X}}_\alpha$.*

Proof. We assume that $\bar{\mathfrak{X}} = \bar{\mathfrak{X}}_\alpha + \bar{\mathfrak{X}}_\beta$, where $\bar{\mathfrak{X}}_\alpha$ is the variety having a simple point at α and $\bar{\mathfrak{X}}_\beta$ is a positive cycle not containing α at all, and let $\bar{F}(U) = \Phi_1(U)\Phi_2(U)$ be the corresponding factorization of the associated form; since $\bar{\mathfrak{X}}_\alpha$ and hence also $\bar{\mathfrak{X}}_\beta$ are rational over $\bar{K}$, the forms $\Phi_1(U)$ and $\Phi_2(U)$ can also be taken to be rational over $\bar{K}$. Since $\bar{\mathfrak{X}}_\alpha$ is simple at the origin α, we can choose the affine coordinate system so that the equations $X_{r+1} = \cdots = X_m = 0$ define the tangential space of $\bar{\mathfrak{X}}_\alpha$ at α. We set ${}_iu_0 = X_i$, ${}_iu_i = 1$, ${}_iu_j = 0$ $(j \neq 0, i)$, for $i = 1, \cdots, m$, and consider the $m-r$ polynomials $\Psi_k(X) = \Phi_1({}_ku, {}_1u, \cdots, {}_ru)$, $k = r+1, \cdots, m$; if we assume for the moment that $\bar{K}$ is infinite, then for a suitable choice of the affine coordinate system in $\bar{S}^m$ we can obtain that the determinant $|\partial\Psi_k(X)/\partial X_j|$, $j, k = r+1, \cdots, m$, does not vanish at α. We set $\phi_k(X) = \bar{F}({}_ku, {}_1u, \cdots, {}_ru) = \Phi_1({}_ku, {}_1u, \cdots, {}_ru)\Phi_2({}_ku, {}_1u, \cdots, {}_ru)$; since the second factor on the right does not vanish at all at α, it follows that the determinant $|\partial\phi_k(X)/\partial X_j|$, $j, k = r+1, \cdots, m$, also does not vanish at α. This shows that the elements $X_1, \cdots, X_r$, $\phi_{r+1}(X), \cdots, \phi_m(X)$ form a minimal basis for $p(\bar{S}/\alpha)$. If we now set $f_k(X) = F({}_ku, {}_1u, \cdots, {}_ru)$,

$k = r + 1, \cdots, m$, then it is easily seen that the polynomials $f_k(X)$ all vanish at every point of $\mathfrak{X}$ and hence are contained in $\mathfrak{P}_v$ (and hence also in $\mathfrak{P}_\alpha$); since we have evidently $\phi_k(X) = \bar{f}_k(X)$ for every k, this shows that the polynomials $\phi_k(X)$ are all in $\bar{\mathfrak{P}}_\alpha$. Since the polynomials $\phi_k(X)$ generate in $\mathfrak{Q}(\bar{S}/\alpha)$ a prime ideal which has the rank $m - r$ and is contained in $\bar{\mathfrak{P}}_\alpha$, and since $\bar{\mathfrak{P}}_\alpha$ has a rank at most $m - r$, it follows that $\bar{\mathfrak{P}}_\alpha$ must coincide with this prime ideal and hence has the polynomials $\phi_k(X)$ as a basis. Finally, since the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha)$ associated with $\bar{\mathfrak{X}}_\alpha$ has the rank $m - r$ and contains $\bar{\mathfrak{P}}_\alpha$, it must coincide with $\bar{\mathfrak{P}}_\alpha$.

In case $\bar{K}$ is finite, we take the ring $K_v[w]$ obtained from K_v by the adjunction of an auxiliary variable w over K, and consider the quotient ring $K_{v,w}$ of $K_v[w]$ with respect to the set $K_v[w] - K_v[w]\pi$; if we denote by $\bar{w}$ the $K_{v,w}\pi$-residue of w, then $\bar{w}$ is a variable over $\bar{K}$, and $\bar{K}(\bar{w})$ is the residue field of $K_{v,w}$. If we replace K_v by $K_{v,w}$ and apply our lemma, and if we denote by $\mathfrak{Q}(\bar{S}/\alpha, \bar{K}(\bar{w}))$ the local ring defined in a similar way as $\mathfrak{Q}(\bar{S}/\alpha)$ with $\bar{K}(\bar{w})$ replacing $\bar{K}$, then we conclude that the ideal $\mathfrak{Q}(\bar{S}/\alpha, \bar{K}(\bar{w}))\bar{\mathfrak{P}}_\alpha$ is the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha, \bar{K}(\bar{w}))$ associated with $\bar{\mathfrak{X}}_\alpha$; since $\bar{\mathfrak{P}}_\alpha$ is the contraction of $\mathfrak{Q}(\bar{S}/\alpha, \bar{K}(\bar{w}))\bar{\mathfrak{P}}_\alpha$ in $\mathfrak{Q}(\bar{S}/\alpha)$, it follows that the ideal $\bar{\mathfrak{P}}_\alpha$ is the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha)$ associated with $\bar{\mathfrak{X}}_\alpha$.

In the next two section we shall be concerned only with those points in S^m (and in $\bar{S}^m$) which are finite with respect to the given affine coordinate system, so that we shall be really dealing with affine varieties and cycles. For the sake of convenience we shall keep the same notations as used before for the entities in the projective space; there will be no danger of confusion, as the context will make it clear what is meant in each case.

2. Consider now a variety V^n in S^m, defined over K, and assume that the specialization $\bar{V}$ of V over v is simple at the point α. Let $\mathfrak{O}$ be the prime ideal in $K[X]$ associated with V, and set $\mathfrak{O}_v = K_v[X] \cap \mathfrak{O}$, $\mathfrak{O}_\alpha = \mathfrak{Q}(S/\alpha)\mathfrak{O}_v$, $R = \mathfrak{Q}(S/\alpha)/\mathfrak{O}_\alpha$, and $\mathfrak{m} = p(S/\alpha)/\mathfrak{O}_\alpha$; then R is a local ring with $\mathfrak{m}$ as the maximal prime ideal, and since $\mathfrak{O}_\alpha$ does not contain any element in K_v, we can embed K_v canonically as a subring in R. Let $\bar{\mathfrak{O}}_\alpha$ be the image ideal of $\mathfrak{O}_\alpha$ under the homomorphism E, and set $\bar{R} = \mathfrak{Q}(\bar{S}/\alpha)/\bar{\mathfrak{O}}_\alpha$; then $\bar{R}$ is a local ring, and since $\bar{\mathfrak{O}}_\alpha$ does not contain any element in $\bar{K}$, we can embed $\bar{K}$ canonically as a subring in $\bar{R}$. It is clear that E induces a homomorphism of R onto $\bar{R}$, which we shall denote by E_R; and if we denote by G and $\bar{G}$ the canonical homomorphisms of $\mathfrak{Q}(S/\alpha)$ onto R and of $\mathfrak{Q}(\bar{S}/\alpha)$ onto $\bar{R}$ respectively, then we have the relation $E_R G = \bar{G} E$. We set $x_i = G(X_i)$ and $\bar{x}_i = \bar{G}(X_i)$ for $i = 1, \cdots, m$; then the point $x = (x_1, \cdots, x_m)$ in S^m is a generic point of V over K and the point $\bar{x} = (\bar{x}_1, \cdots, \bar{x}_m)$ is a generic point over $\bar{K}$ of the component $\bar{V}_\alpha$ of $\bar{V}$ containing α, and it is clear that $\bar{x}$ is the image of x under the homomorphism E_R. According to Lemma 1 above, applied to V as a prime cycle in S^m, the ideal $\bar{\mathfrak{D}}_\alpha$ is the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha)$ associated with $\bar{V}_\alpha$; since $\bar{V}_\alpha$ is simple at α, this means that $\bar{R}$ is a regular local ring of dimension n. If now $y_1, \cdots, y_n$ are elements in R such that their images $\bar{y}_1, \cdots, \bar{y}_n$ under E_R form a minimal basis for the maximal prime ideal $\bar{\mathfrak{m}}$ in $\bar{R}$, then it is easily seen that the $n+1$ elements $\pi, y_1, \cdots, y_n$ will form a basis for the maximal prime ideal $\mathfrak{m}$ in R; since R has the dimension at least $n+1$, this shows that this basis is minimal and that R is a regular local ring of dimension $n+1$.

We consider the (affine) coordinate ring $K[x]$ of V, and the subring $K_v[x]$ contained in it; it is clear that $K[x]$ is the quotient ring of $K_v[x]$ with respect to the multiplicatively closed set of all non-zero elements in K_v. Let $\mathfrak{i}$ be an ideal in $K_v[x]$, and let $\mathfrak{p}_i$, $i=1, \cdots, c$, be the minimal prime divisors of $\mathfrak{i}$; then, for each $\mathfrak{p}_i$ which does not contain any element in K_v (i. e. $K[x]\mathfrak{p}_i \neq K[x]$), the ideal $K[x]\mathfrak{p}_i$ is a minimal prime divisor of the ideal $K[x]\mathfrak{i}$, and in this way we obtain all the minimal prime divisors of $K[x]\mathfrak{i}$. It is well-known that if the ideal $\mathfrak{i}$ is the contraction of an ideal in $K[x]$, then none of the ideals $\mathfrak{p}_i$ can contain any element in K_v and $K[x]\mathfrak{i}$ is the only ideal in $K[x]$ which contracts to $\mathfrak{i}$ in $K_v[x]$. If we denote by W and W_i the subsets in V (or rather in the part of V which is finite with respect to the given affine coordinate system) defined by the ideals $\mathfrak{i}$ and $\mathfrak{p}_i$ respectively (or by $K[x]\mathfrak{i}$ and $K[x]\mathfrak{p}_i$ respectively), then each W_i is an affine K-variety and we have the equation $W = \bigcup_i W_i$; it is clear that if $\mathfrak{i}$ is the contraction of an ideal in $K[x]$, then none of the sets W_i is empty.

Consider now the coordinate ring $\bar{K}[\bar{x}]$ of the variety $\bar{V}_\alpha$, and denote by E' the homomorphism of $K_v[x]$ onto $\bar{K}[\bar{x}]$ which is the restriction to $K_v[x]$ of E_R (E' is also an extension of the canonical homomorphism E of K_v onto $\bar{K}$); we observe that the kernel of E' is the ideal $K_v[x]\pi$. We denote by $\bar{\mathfrak{i}}$ and $\bar{\mathfrak{p}}_i$ the image ideals of $\mathfrak{i}$ and $\mathfrak{p}$ respectively under E'; we have evidently the relation $\bar{\mathfrak{i}} \subset \bar{\mathfrak{p}}_i$. On the other hand, if f_i are elements in $\mathfrak{p}_i$ such that their images $\bar{f}_i$ under E' all coincide with one element ϕ in $\bigcap_i \bar{\mathfrak{p}}_i$, then the element $\prod_i f_i$ is in the radical of $\mathfrak{i}$; since the image of the radical of $\mathfrak{i}$ under E' is contained in the radical of $\bar{\mathfrak{i}}$, this means that a power of the element ϕ is in the radical of $\bar{\mathfrak{i}}$, and hence ϕ is itself in the radical of $\bar{\mathfrak{i}}$; this shows that $\bigcap_i \bar{\mathfrak{p}}_i$ is contained in the radical of $\bar{\mathfrak{i}}$. If we denote by $\bar{W}_i$ the subsets in $\bar{V}_\alpha$ defined by the ideals $\bar{\mathfrak{p}}_i$, then it follows from what we have just said that the union $\bigcup_i \bar{W}_i$ is precisely the subset in $\bar{V}_\alpha$ defined by the ideal $\bar{\mathfrak{i}}$. Now, for each $\mathfrak{p}_i$ which does not contain any element in K_v (and hence W_i is not empty), the set $\bar{W}_i$ is by definition the specialization of the set W_i over E (or over the valuation v); hence the set $\bar{W} = \bigcup_i{}' \bar{W}_i$, where the symbol $\bigcup{}'$ indicates that the union is taken over all i such that $\mathfrak{p}_i$ does not contain any non-zero element in K_v, is the specialization of W over E.

Now, the point α in $\bar{V}_\alpha$ is the only zero of the ideal $\bar{K}[\bar{x}] \cap \bar{\mathfrak{m}}$, and $\bar{R}$ is the quotient ring of $\bar{K}[\bar{x}]$ with respect to $\bar{K}[\bar{x}] - (\bar{K}[\bar{x}] \cap \bar{\mathfrak{m}})$; it follows that α is contained in $\bar{W}$ if and only if for at least one i the ideal $\bar{R}\bar{\mathfrak{p}}_i$ is not the unit ideal and the ideal $\mathfrak{p}_i$ does not contain any non-zero element in K_v. Since $\bar{R}\bar{\mathfrak{p}}_i$ is clearly the image of $R\mathfrak{p}_i$ under E_R, it follows that α is contained in $\bar{W}$ if and only if for at least one i the ideal $R\mathfrak{p}_i$ does not contain any non-zero element in K_v, and it is easily seen that this is so if and only if the ideal $R\mathfrak{i}$ does not contain any non-zero element in K_v.

We shall say that the point α is an *isolated* zero of the ideal $\bar{\mathfrak{i}}$ if the ideal $\bar{R}\bar{\mathfrak{i}}$ is primary for the ideal $\bar{\mathfrak{m}}$, and the isolated zero α of $\bar{\mathfrak{i}}$ is said to be a *simple* zero of $\bar{\mathfrak{i}}$ if $\bar{R}\bar{\mathfrak{i}} = \bar{\mathfrak{m}}$.

THEOREM 1. *If the point α is an isolated zero of $\bar{\mathfrak{i}}$ and if $R\mathfrak{i}$ has a rank at most n, then α is contained in $\bar{W}$; furthermore, if K_v is complete and if α is a simple zero of $\bar{\mathfrak{i}}$, then there is exactly one point a in W which specializes over E to α, and this point a is rational over K_v and is a simple zero of $\mathfrak{i}$.*

Proof. To prove that α is contained in $\bar{W}$, we have to show that the ideal $R\mathfrak{i}$ does not contain any non-zero element in K_v; we assume that $\bar{R}\bar{\mathfrak{i}}$ is primary for $\bar{\mathfrak{m}}$ and the $R\mathfrak{i}$ contains a non-zero element in K_v, and we shall show that $R\mathfrak{i}$ must then have the rank $n+1$. In fact, for every i, the prime ideal $R\mathfrak{p}_i \cap K_v$ in K_v is in this case not the zero ideal and hence must coincide with the ideal $K_v\pi$; it follows that every ideal $R\mathfrak{p}_i$ contains the kernel $R\pi$ of E_R and hence must coincide with the inverse image under E_R of the ideal $\bar{R}\bar{\mathfrak{p}}_i$. Since $\bar{R}\bar{\mathfrak{i}}$ is primary for $\bar{\mathfrak{m}}$, every ideal $\bar{R}\bar{\mathfrak{p}}_i$ is primary for $\bar{\mathfrak{m}}$; it follows that every ideal $R\mathfrak{p}_i$ is primary for $\mathfrak{m}$ and hence has the rank $n+1$, and this implies that $R\mathfrak{i}$ has also the rank $n+1$.

If $\bar{R}\bar{\mathfrak{i}} = \bar{\mathfrak{m}}$, then we have the relation $R(\mathfrak{i}, \pi) = \mathfrak{m}$. Consider now the residue ring $T = R/R\mathfrak{i}$, which is a local ring with the maximal prime ideal $\mathfrak{m}/R\mathfrak{i}$; since $R\mathfrak{i}$ does not contain any non-zero element in K_v, we can embed K_v canonically in T as a subring. It is clear that T and K_v have the same residue field K, and the relation $\mathfrak{m}/R\mathfrak{i} = R(\mathfrak{i}, \pi)/R\mathfrak{i}$ shows that the maximal prime ideal of the so embedded ring K_v generates in T the maximal prime ideal of T. If K_v is complete, then it follows from a well-known result that

T coincides with its subring K_v. Since $T = K_v$ is an integral domain, $R\mathfrak{i}$ is a prime ideal, and hence we have $c = 1$ and $R\mathfrak{i} = R\mathfrak{p}_1$; since the quotient ring of $K_v[x]$ with respect to the set $K_v[x] - \mathfrak{p}_1$ coincides with the quotient ring of R with respect to the set $R - R\mathfrak{p}_1 = R - R\mathfrak{i}$, we can identify T with the residue ring $K_v[x]/\mathfrak{p}_1$, so that $K_v[x]/\mathfrak{p}_1$ also coincides with K_v. There exists therefore a homomorphism H of $K_v[x]$ onto K_v which leaves every element in K_v invariant and whose kernel is the ideal $\mathfrak{p}_1$; if we set $a_i = H(x_i)$, $i = 1, \cdots, m$, then the point $a = (a_1, \cdots, a_m)$ in V is clearly the only zero of $\mathfrak{p}_1$, and since the point a has a unique image $\bar{a}$ under E and has the point α as a specialization over E, we must have the equality $\bar{a} = \alpha$. Thus the rational point a is the only point in W which can specialize over E to the point α, and it can specialize over E only to α. Finally, it is clear that $K[x]\mathfrak{p}_1$ is the defining prime ideal of the point a in $K[x]$, and that the quotient ring of $K[x]$ with respect to the set $K[x] - K[x]\mathfrak{p}_1$ coincides with the quotient ring of $K_v[x]$ with respect to the set $K_v[x] - \mathfrak{p}_1$, which in turn coincides with the quotient ring of R with respect to the set $R - R\mathfrak{p}_1$; it follows then from the relation $R\mathfrak{i} = R\mathfrak{p}_1$ that the point a is a simple zero of $\mathfrak{i}$. This concludes the proof of our theorem.

As a corollary of the above theorem we obtain a result which can be considered as a generalization of the well-known Hensel's Lemma:[6]

COROLLARY. *Let K be a field which is complete with respect to a real discerte valuation v, let V be a variety in S^m defined over K, and let $\bar{V}$ be its specialization over v; if α is a point in $\bar{V}$ such that α is rational over $\bar{K}$ and $\bar{V}$ is simple at α, then there exists a point a in V such that a is rational over K_v, V is simple at a, and $\bar{a} = \alpha$.*

In fact, if $y_1, \cdots, y_n$ are elements in R such that their images $\bar{y}_1, \cdots, \bar{y}_n$ under E_R form a basis for $\bar{\mathfrak{m}}$, then we can take for $\mathfrak{i}$ the ideal in $K_v[x]$ generated by the elements $y_1, \cdots, y_n$, which has a rank at most n; our corollary then follows immediately from Theorem 1.

3. Let $\boldsymbol{x} = (x^{(1)}, \cdots, x^{(d)})$ be a system of d points in W, which for the sake of convenience we shall assume to be distinct. A system of d (not necessarily distinct) points $\boldsymbol{\beta} = (\beta^{(1)}, \cdots, \beta^{(d)})$ in $\bar{V}_\alpha$ is said to be a specialization of the system $\boldsymbol{x}$ over E if the mapping $x^{(i)} \to \beta^{(i)}$ defines an extension of E to a homomorphism E_0 of the ring $K_v[\boldsymbol{x}]$ onto the ring $\bar{K}[\boldsymbol{\beta}]$. The number of times the point α appears in the system $\boldsymbol{\beta}$ is then called the multiplicity of α in the specialization $\boldsymbol{\beta}$ of $\boldsymbol{x}$ over E. It is clear that in order that this multiplicity can be positive, it is necessary that α is not only a zero of the ideal $\bar{\mathfrak{i}}$, but also contained in the set $\bar{W}$; as we have seen above, this condition is equivalent to the condition that the ideal $R\mathfrak{i}$ does not contain any element in K_v.

---

[6] Such a generalization of Hensel's Lemma was conjectured by A. Weil some years ago; a special case of it, namely, for the Jacobian variety of a curve, has been recently proved by A. P. Mattuck in an unpublished manuscript.

THEOREM 2. *If the point α is a simple isolated zero of $\bar{\mathfrak{i}}$, then the multiplicity of α in any specialization over E of any system of points in W is at most equal to* 1.

Proof. If K_v is complete, then this theorem follows immediately from Theorem 1; for then the point a is the only point in W which specializes over E to α, and hence α appears in $\boldsymbol{\beta}$ if and only if a appears in $\boldsymbol{x}$ (observe that, since the points in $\boldsymbol{x}$ are assumed to be distinct, a can only appear once in $\boldsymbol{x}$). In order to prove our theorem it is sufficient to show that the homomorphism E_0 can be extended to a homomorphism of $K_v^*[\boldsymbol{x}]$ onto $\bar{K}[\boldsymbol{\beta}]$, where K_v^* denotes the completion of K_v. Since $\bar{K}[\boldsymbol{\beta}]$ is an integral domain, the kernel $\mathfrak{r}_0$ of E_0 is a prime ideal, and E_0 can be extended to a homomorphism E_1 of the quotient ring N_1 of $K_v[\boldsymbol{x}]$ with respect to the set $K_v[\boldsymbol{x}]-\mathfrak{r}_0$ onto the field $\bar{K}(\boldsymbol{\beta})$; since the contraction of $\mathfrak{r}_0$ in K_v is evidently the kernel $K_v\pi$ of E, it follows that $K_v=N_1\cap K$. Let N_1 be embedded in a complete local domain N_2 which dominates N_1 (i.e. N_2 contains N_1 and its maximal prime ideal contract in N_1 to the maximal prime ideal of N_1) and whose residue field coincides with the residue field $\bar{K}(\boldsymbol{\beta})$ of N_1; for example, we can take N_2 to be the residue ring of the completion of N_1 modulo a minimal prime divisor of its zero ideal. The canonical homomorphism E_2 of N_2 onto its residue field $\bar{K}(\boldsymbol{\beta})$ is then an extension of E_1. Since N_2 contains K_v and is complete, we can embed the completion K_v^* of K_v in N_2, and E_2 evidently induces a homomorphism of $K_v^*[\boldsymbol{x}]$ onto $\bar{K}[\boldsymbol{\beta}]$ which is an extension of E_0.

We consider now the positive cycle $\mathfrak{X}$ introduced in Section 1, and assume that the variety V contains $\mathfrak{X}$ so that $\mathfrak{P}$ contains $\mathfrak{O}$ and hence also $\mathfrak{P}_a$ contains $\mathfrak{O}_a$. Let $\mathfrak{p}$ be the image ideal of $\mathfrak{P}_a$ under the homomorphism G, and let $\bar{\mathfrak{p}}$ be the image of $\mathfrak{P}_a$ under the homomorphism $\bar{G}$; then both ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ will have ranks at most $n-r$, and $\bar{\mathfrak{p}}$ is the image of $\mathfrak{p}$ under the homomorphism E_R. Since $\bar{V}_a$ contains $\bar{\mathfrak{X}}_a$, the tangential space of $\bar{V}_a$ at α contains the tangential space of $\mathfrak{X}_a$ at α; by a suitable choice of the affine coordinate system, we can assume that the equations $X_{n+1}=\cdots=X_m=0$ defines the tangential space of $\bar{V}_a$ at α. Then, as in the proof of Lemma 1, the ideal $\bar{\mathfrak{O}}_a$ has a basis $\omega_{n+1}(X),\cdots,\omega_m(X)$, in $\bar{K}[X]$, such that $X_1,\cdots,X_n$, $\omega_{n+1}(X),\cdots,\omega_m(X)$ form a minimal basis for

$p(\bar{S}/\alpha)$; using the determinant criterion for the minimal basis, one sees readily that the basis $\phi_{r+1}(X), \cdots, \phi_m(X)$ of $\mathfrak{P}_\alpha$ can be so chosen that $\phi_i(X) = \omega_i(X)$ for $i = n+1, \cdots, m$. Going over to the images in $\bar{R}$, under the homomorphism $\bar{G}$ and observing that $\bar{K}$ remains invariant under $\bar{G}$, this means that the ideal $\bar{\mathfrak{p}}$ has a basis $\phi_{r+1}(\bar{x}), \cdots, \phi_n(\bar{x})$ which can be extended to a minimal basis $\bar{x}_1, \cdots, \bar{x}_r$, $\phi_{r+1}(\bar{x}), \cdots, \phi_n(\bar{x})$ for $\bar{\mathfrak{m}}$. Let $f_k(X)$, $k = r+1, \cdots, m$, be elements in $\mathfrak{P}_\alpha$ such that $\bar{f}_k(X) = \phi_k(X)$ for every k and that $f_{n+1}(X), \cdots, f_m(X)$ are in $\mathfrak{O}_\alpha$; then $f_{n+1}(x) = \cdots = f_m(x) = 0$ and the elements $f_{r+1}(x), \cdots, f_n(x)$ are in $\mathfrak{p}$, with $\phi_{r+1}(\bar{x}), \cdots, \phi_n(\bar{x})$ as their respective images under E_R. Since the elements π, $x_1, \cdots, x_r$, $f_{r+1}(x), \cdots, f_n(x)$ clearly generate the ideal $\mathfrak{m}$, they must form a minimal basis for $\mathfrak{m}$; this shows that the elements $f_{r+1}(x), \cdots, f_n(x)$ generate a prime ideal of rank $n-r$ in R, and since $\mathfrak{p}$ has a rank at most $n-r$, this prime ideal must coincide with $\mathfrak{p}$. We observe also that since the elements $f_{r+1}(X), \cdots, f_m(X)$ can be extended to a minimal basis for $p(S/\alpha)$, by adding the elements π, $X_1, \cdots, X_r$, they generate a prime ideal of rank $m-r$ and hence must form a basis for $\mathfrak{P}_\alpha$.

Now, let $\mathfrak{Y}^s$ $(s = n-r)$ be another positive cycle contained in the variety V, and assume that $\mathfrak{Y}$ is rational over K and that the specialization $\bar{\mathfrak{Y}}$ of $\mathfrak{Y}$ over v is also simple at α; we denote by $\mathfrak{Q}$, $\mathfrak{Q}_v$, $\mathfrak{Q}_\alpha$, and $\mathfrak{q}$ the ideals having the same meanings for the cycle $\mathfrak{Y}$ as the ideals $\mathfrak{P}$, $\mathfrak{P}_v$, $\mathfrak{P}_\alpha$, and $\mathfrak{p}$ respectively for the cycle $\mathfrak{X}$. Then there exists a basis $\theta_{s+1}(X), \cdots, \theta_m(X)$ in $\bar{K}[X]$ for $\bar{\mathfrak{Q}}_\alpha$ such that $\theta_i(X) = \omega_i(X)$ for $i = n+1, \cdots, m$, and such that $\theta_{s+1}(\bar{x}), \cdots, \theta_n(\bar{x})$ form a basis for $\bar{\mathfrak{q}}$ which can be extended to a minimal basis for $\bar{\mathfrak{m}}$. The condition that $\bar{\mathfrak{X}}$ and $\bar{\mathfrak{Y}}$ are transversal to each other at α in $\bar{V}$ is equivalent to the condition that the elements $\phi_{r+1}(\bar{x}), \cdots, \phi_n(\bar{x})$, $\theta_{s+1}(\bar{x}), \cdots, \theta_n(\bar{x})$ form a minimal basis for $\bar{\mathfrak{m}}$. If this is the case, and if we take elements $g_{s+1}(X), \cdots, g_n(X)$ in $\mathfrak{Q}_\alpha$ such that $\bar{g}_j(X) = \theta_j(X)$ for every j, then $g_{s+1}(x), \cdots, g_n(x)$ form a basis for $\mathfrak{q}$, and the elements π, $f_{r+1}(x), \cdots, f_n(x)$, $g_{s+1}(x), \cdots, g_n(x)$ form a minimal basis for $\mathfrak{m}$; this show that the ideal $(\mathfrak{p}, \mathfrak{q})$ has the rank n (and is in fact a prime ideal). If we now apply Theorems 1 and 2 by taking for $\mathfrak{i}$ the restriction of the ideal $(\mathfrak{p}, \mathfrak{q})$ in $K_v[x]$, we obtain then the following theorem, which is the well-known criterion for unit multiplicity in a somewhat more precise version.

THEOREM 3. *Let* V^n *be a variety in* S^m, *defined over* K, *and let* $\mathfrak{X}^r$ *and* $\mathfrak{Y}^s$ $(r+s=n)$ *be two positive cycles in* V, *rational over* K; *let* v *be a real discrete valuation of* K, *and let* $\bar{V}$, $\bar{\mathfrak{X}}$, *and* $\bar{\mathfrak{Y}}$ *be the specializations of* V, $\mathfrak{X}$, *and* $\mathfrak{Y}$ *respectively over* v. *If* α *is a rational point over* $\bar{K}$ *in* $\bar{V}$ *such that* $\bar{V}$ *is simple at* α *and that* $\bar{\mathfrak{X}}$ *and* $\bar{\mathfrak{Y}}$ *are transversal to each other at* α, *then* α *has the multiplicity* 1 *in the specialization over* v *of every system of points in* $|\mathfrak{X}| \cap |\mathfrak{Y}|$ *which includes all the isolated points in* $|\mathfrak{X}| \cap |\mathfrak{Y}|$. *If furthermore* K *is complete with respect to* v, *then there is exactly one point* a *in* $|\mathfrak{X}| \cap |\mathfrak{Y}|$ *which specializes to* α *over* v; *and this point* a *is rational over* K_v (*hence* $\bar{a} = \alpha$), V *is simple at* a, *and* $\mathfrak{X}$ *and* $\mathfrak{Y}$ *are transversal to each other at* a.

4. In the above treatment of the criterion for unit multiplicity, we have kept our arguments on as elementary a level as possible, in consonant with the foundational nature of our purpose. In fact, the greater part of our argument consists of a precise local formulation of the various geometric concepts involved in this criterion; the actual proof of the criterion itself is very short and is contained essentially in the proof of Theorem 1. If we now take a more sophisticated point of view and assume a knowledge of the intersection-theory, then the criterion for unit multiplicity, in the present version as an assertion on the specialization-multiplicity, is really only a special case of a more general theorem on the invariance of intersection-multiplicity under specialization, and there naturally arises the question whether, corresponding to Theorem 3, we can also prove a more precise version of this invariance theorem. In the following we shall show that this can be done, by using the Chevalley-Samuel-Nagata theory of multiplicity in a local ring. We shall need some of the results in the paper of Nagata cited before.[5]

As in Section 1, we consider the positive r-cycle $\mathfrak{X}$ in S^m, except that we shall now no longer assume that $\mathfrak{X}$ is simple at the point α; for the sake of simplicity, we shall assume that $\mathfrak{X}$ is a prime rational cycle over K_v (so that $\mathfrak{P}_v$ and hence $\mathfrak{P}_\alpha$ are prime ideals). Let Ω_0 be a prime rational r-cycle over $\bar{K}$ in $\bar{S}^m$ which contains the point α and whose support is contained in the support of $\bar{\mathfrak{X}}$, and let $\Phi_0(U)$ be the associated form of Ω_0; we set $\bar{\mathfrak{X}} = \Omega_1 + \Omega_2$, where Ω_1 is a positive r-cycle with the same support as Ω_0 and Ω_2 is a positive cycle relatively prime to Ω_0, and let $\bar{F}(U) = \Phi_1(U)\Phi_2(U)$ be the corresponding factorization of $\bar{F}(U)$. Let d_0 and d_1 be the degrees of $\Phi_0(U)$ and $\Phi_1(U)$ respectively; the number d_1/d, which will presently be shown to be an integer, is the coefficient of Ω_0 as a component in $\bar{\mathfrak{X}}$ and will be denoted by $\mu(\Omega_0, \bar{\mathfrak{X}})$. Let $\bar{\mathfrak{A}}$ be the prime ideal in $\mathfrak{Q}(\bar{S}/\alpha)$ associated with Ω_0, and let $\mathfrak{A} = E^{-1}(\bar{\mathfrak{A}})$ be the corresponding prime ideal in $\mathfrak{Q}(S/\alpha)$; then $\mathfrak{A}$ is a minimal prime divisor of the ideal $(\pi, \mathfrak{P}_\alpha)$ in $\mathfrak{Q}(S/\alpha)$, and in this way all the minimal prime divisors of $(\pi, \mathfrak{P}_\alpha)$ can be obtained.

LEMMA 2. $\mu(\Omega_0, \bar{\mathfrak{X}}) = e((\pi, \mathfrak{P}_\alpha)\mathfrak{Q}(S/\alpha)_{\mathfrak{A}}/\mathfrak{P}_\alpha\mathfrak{Q}(S/\alpha)_{\mathfrak{A}})$.

Proof. Let ${}_iw_j$, $i=1,\cdots,r$, and $j=0,1,\cdots,m$, be $r(m+1)$ independent variables over K_v; we set ${}_iw=({}_iw_0,{}_iw_1,\cdots,{}_iw_m)$ and denote by w the set of all $r(m+1)$ variables ${}_iw_j$. We set $F({}_0U,w)=F({}_0U,{}_1w,\cdots,{}_rw)$, and similarly for other associated forms; we denote by $K_{v,w}$ the quotient ring of $K_v[w]$ with respect to the prime ideal generated in it by π, so that $K_{v,w}$ is a real discrete valuation ring; and we observe that if we denote by $\bar{w}$ the image of w in the residue field of $K_{v,w}$, then $\bar{w}$ is a set of independent variable over $\bar{K}$ and $\bar{K}(\bar{w})$ is this residue field. We set $L_i={}_iw_0+\sum_{j=1}^{m}{}_iw_jX_j$ and denote by $\mathfrak{O}(S/\alpha,K_{v,w})$ the local ring defined in the same way as $\mathfrak{O}(S/\alpha)$ but with $K_{v,w}$ replacing K_v; we set

$$M=\mathfrak{O}(S/\alpha)\mathfrak{P}_\alpha,\quad \mathfrak{g}=\mathfrak{A}/\mathfrak{P}_\alpha\quad N=\mathfrak{O}(S/\alpha,K_{v,w})/(\mathfrak{P}_\alpha,L_1,\cdots,L_r),$$

and

$$\mathfrak{h}=\mathfrak{A}\mathfrak{O}(S/\alpha,K_{v,w})/(\mathfrak{P}_\alpha,L_1,\cdots,L_r).$$

Then it is easily seen that $N_{\mathfrak{h}}$ can be obtained from $M_{\mathfrak{g}}$ by first adjoining the rm variables ${}_iw_j$, $j\neq 0$, and then forming the quotient ring of the so obtained ring with respect to the ideal generated in it by $\mathfrak{g}$. It follows that $e(\pi N_{\mathfrak{h}})=e(\pi M_{\mathfrak{g}})=e((\pi,\mathfrak{P}_\alpha)\mathfrak{O}(S/\alpha)_{\mathfrak{A}}/\mathfrak{P}_\alpha\mathfrak{O}(S/\alpha)_{\mathfrak{A}})$. Since $N_{\mathfrak{h}}{}^*$ is a finite module over $K_{v,w}{}^*$, it follows by a well-known argument[7] using the decomposition of the ideal $\mathfrak{h}N_{\mathfrak{h}}{}^*$ that

$$e(\pi N_{\mathfrak{h}})=e(\pi N_{\mathfrak{h}}{}^*)=l(N_{\mathfrak{h}}{}^*/\pi N_{\mathfrak{h}}{}^*)=[N_{\mathfrak{h}}{}^*:K_{v,w}{}^*]/[N_{\mathfrak{h}}/\mathfrak{h}:\bar{K}(\bar{w})].$$

It is easily verified that $[N_{\mathfrak{h}}/\mathfrak{h}:\bar{K}(\bar{w})]$ is equal to the degree of the form $\Phi_0({}_0U,\bar{w})$ and hence is equal to d_0. In order to complete the proof of our lemma, it remains to show that $[N_{\mathfrak{h}}{}^*:K_{v,w}{}^*]=d_1$. This can be done by generalizing the usual argument in the ramification theory, first observing that[8] there exists a factorization $F({}_0U,w)=F_1({}_0U)F_2({}_0U)$ in $K_{v,w}{}^*[{}_0U]$ corresponding to the factorization $\bar{F}({}_0U,\bar{w})=\Phi_1({}_0U,\bar{w})\Phi_2({}_0U,\bar{w})$, and then showing that the number $[N_{\mathfrak{h}}{}^*:K_{v,w}{}^*]$ is equal to the degree of the form $F_1({}_0U)$, which is the same as the degree d_1 of $\Phi_1({}_0U,\bar{w})$.

Let A_i be the components in the positive cycle $\bar{\mathfrak{X}}$ which contain the point α, let $\bar{\mathfrak{A}}_i$ be the prime ideals in $\mathfrak{O}(\bar{S}/\alpha)$ associated with A_i, and let $\mathfrak{A}_i=E^{-1}(\bar{\mathfrak{A}}_i)$ be the corresponding minimal prime divisor of the ideal $(\pi,\mathfrak{P}_\alpha)$ in $\mathfrak{O}(S/\alpha)$. If we denote by $\mathfrak{a}_i$ the image ideals of $\mathfrak{A}_i$ in R under the homomorphism G, then it is easily seen that the ideals $\mathfrak{a}_i$ are the minimal prime divisors of the ideal $(\pi, \mathfrak{p})R$, and we have the equality $e((\pi, \mathfrak{p})R_{\mathfrak{a}_i}/\mathfrak{p}R_{\mathfrak{a}_i}) = e((\pi, \mathfrak{P}_{\mathfrak{a}})\mathfrak{Q}(S/\alpha)_{\mathfrak{A}_i}/\mathfrak{P}_{\mathfrak{a}}\mathfrak{Q}(S/\alpha)_{\mathfrak{A}_i})$. It follows then from Lemma 2 that $\mu(\mathrm{A}_i, \bar{\mathfrak{X}}) = \mathrm{e}((\pi, \mathfrak{p})R_{\mathfrak{a}_i}/\mathfrak{p}R_{\mathfrak{a}_i})$. For each i, let $\mathfrak{a}_{ij}$ be the minimal prime divisors of $\mathfrak{a}_i R^*$; since $\mathfrak{a}_i$ is analytically unramified (for $R/\mathfrak{a}_i$ is a "geometrical" local ring), we have the equality

---

[7] See e. g. C. Chevalley, "On the Theory of Local Rings," *Annals of Mathematics*, vol. 44 (1943), pp. 690-708, § IV, Lemma 2.

[8] See Lemma 1 in our recent paper "On the Principle of Degeneration in Algebraic Geometry," *Annals of Mathematics*, vol. 66 (1957), pp. 70-79.

$$e((\pi, \mathfrak{p})R^*_{\mathfrak{a}_{ij}}/\mathfrak{p}R^*_{\mathfrak{a}_{ij}}) = e((\pi, \mathfrak{p})R_{\mathfrak{a}_i}/\mathfrak{p}R_{\mathfrak{a}_i}).$$

We consider now, as in Section 3, two positive cycles $\mathfrak{X}^r$ and $\mathfrak{Y}^s$ in a variety V^n $(n = r + s)$, and we shall use the same notation as developed there; while $\bar{V}$ is still assumed to be a variety which is simple at the point α, we shall assume no longer that $\bar{\mathfrak{X}}$ or $\bar{\mathfrak{Y}}$ is simple at α, nor that they are transversal to each other. Instead, we shall only assume that $\bar{\mathfrak{X}}$ and $\bar{\mathfrak{Y}}$ intersect properly at α, which is equivalent to assuming that the ideal $(\bar{\mathfrak{p}}, \bar{\mathfrak{q}})$ is primary for $\bar{\mathfrak{m}}$; this latter assertion follows from the fact that the radical of the ideal $\bar{\mathfrak{p}}$ (or $\bar{\mathfrak{q}}$) is the ideal associated with the support of $\bar{\mathfrak{X}}$ (or $\bar{\mathfrak{Y}}$), and this fact can be easily proved by a method similar to that used in the proof of Lemma 1. Since $(\bar{\mathfrak{p}}, \bar{\mathfrak{q}})$ has the rank n, the ideal $(\mathfrak{p}, \mathfrak{q})$ must have at least the same rank n, and since R is an unramified regular local ring, the rank of $(\mathfrak{p}, \mathfrak{q})$ must be equal to n. Let $\mathfrak{e}_i$ be the minimal prime divisors of the ideal $(\mathfrak{p}, \mathfrak{q})R^*$. Consider the residue ring $T_i = R^*/\mathfrak{e}_i$; it is clear that $K_v{}^*$ can be embedded canonically in T_i as a subring. In fact, T_i is a finite module over $K_v{}^*$, and we have the equality $[T_i : K_v{}^*] = e((\pi, \mathfrak{e}_i)R^*/\mathfrak{e}_i)$. If we denote by H_i the canonical homomorphism of R^* onto $R^*/\mathfrak{e}_i$ and set $a^{(i)}{}_j = H_i(x_j)$, then it can be shown exactly as in Section 3 that the point $a^{(i)} = (a^{(i)}{}_1, \cdots, a^{(i)}{}_m)$ is an intersection point of $\mathfrak{X}$ and $\mathfrak{Y}$; and if we denote by $\mathfrak{Z}_i$ the 0-cycle consisting of the complete set of conjugates of the point $a^{(i)}$ over $K_v{}^*$, then $\mathfrak{Z}_i$ is evidently rational over $K_v{}^*$ and its specialization $\bar{\mathfrak{Z}}_i$ is the cycle consisting of the point α with the coefficient $e((\pi, \mathfrak{e}_i)R^*/\mathfrak{e}_i)$. We set $\mathfrak{Z} = \sum_i i(\mathfrak{Z}_i; \mathfrak{X} \cdot \mathfrak{Y}) \cdot \mathfrak{Z}_i$; then a point a in $|\mathfrak{X}| \cap |\mathfrak{Y}|$ will specialize to α over the specialization $(\mathfrak{X}, \mathfrak{Y}) \rightarrow (\bar{\mathfrak{X}}, \bar{\mathfrak{Y}})$ if and only if the coefficient $\mu(a, \mathfrak{Z})$ of a in $\mathfrak{Z}$ is positive. We shall now show that $\deg \mathfrak{Z} = i(\alpha; \bar{\mathfrak{X}} \cdot \bar{\mathfrak{Y}})$.

Let R' be another copy of the local ring R, but with the same basic ring K_v, and let a prime be used to denote generally the corresponding entities in R'; we consider the complete tensor product J of R and R' (or of R^* and R'^*) over $K_v{}^*$ and denote by $\mathfrak{d}$ the ideal in J generated by the n elements $x_1 - x_1', \cdots, x_n - x_n'$. It is well-known that the prime ideals $(\mathfrak{d}, \mathfrak{e}_i)J$ are precisely the minimal prime divisors of the ideal $(\mathfrak{d}, \mathfrak{p}, \mathfrak{q}')J$, and hence the ideals $(\mathfrak{d}, \mathfrak{e}_i)J/(\mathfrak{p}, \mathfrak{q}')J$ are the minimal prime divisors of the ideal $(\mathfrak{d}, \mathfrak{p}, \mathfrak{q}')J/(\mathfrak{p}, \mathfrak{q}')J$ in the local ring $J/(\mathfrak{p}, \mathfrak{q}')J$. Applying the Associativity Formula, we obtain the equation

$$
\begin{aligned}
& e((\mathfrak{d},\pi,\mathfrak{p},\mathfrak{q}')J/(\mathfrak{p},\mathfrak{q}')J)\\
(1)\qquad & =\sum_i e((\mathfrak{d},\mathfrak{p},\mathfrak{q}')J_{(\mathfrak{d},\mathfrak{e}_i)}/(\mathfrak{p},\mathfrak{q}')J_{(\mathfrak{d},\mathfrak{e}_i)})\cdot e((\mathfrak{d},\pi,\mathfrak{e}_i)J/(\mathfrak{d},\mathfrak{e}_i)J)\\
& =\sum_i e((\mathfrak{d},\mathfrak{p},\mathfrak{q}')J_{(\mathfrak{d},\mathfrak{e}_i)}/(\mathfrak{p},\mathfrak{q}')J_{(\mathfrak{d},\mathfrak{e}_i)})\cdot e((\pi,\mathfrak{e}_i)R^*/\mathfrak{e}_iR^*)\\
& =\sum_i i(\mathfrak{Z}_i;\mathfrak{X}\cdot\mathfrak{Y})\cdot\deg\mathfrak{Z}_i=\deg\mathfrak{Z}.
\end{aligned}
$$

Let B_k be the components in $\bar{Y}$ which contain the point α, and let $\mathfrak{b}_k$ and $\mathfrak{b}_{kl}$ have the same meanings with respect to B_k as $\mathfrak{a}_i$ and $\mathfrak{a}_{ij}$ have with respect to A_i; then it can be easily seen that the ideals $\mathfrak{c}_{ij,kl}=(\mathfrak{a}_{ij},\mathfrak{b}_{kl}')J$ are the minimal prime divisors of the ideal $(\pi,\mathfrak{p},\mathfrak{q}')J$, and we have the relation

$$
\begin{aligned}
e((\pi,\mathfrak{p},\mathfrak{q}')J_{\mathfrak{c}_{ij,kl}}/(\mathfrak{p},\mathfrak{q}')J_{\mathfrak{c}_{ij,kl}}) &= e((\pi,\mathfrak{p})R^*{}_{\mathfrak{a}_{ij}}/\mathfrak{p}R^*{}_{\mathfrak{a}_{ij}})\cdot e((\pi,\mathfrak{q})R^*{}_{\mathfrak{b}_{kl}}/\mathfrak{q}R^*{}_{\mathfrak{b}_{kl}})\\
&= e((\pi,\mathfrak{p})R_{\mathfrak{a}_i}/\mathfrak{p}R_{\mathfrak{a}_i})\cdot e((\pi,\mathfrak{q})R_{\mathfrak{b}_k}/\mathfrak{q}R_{\mathfrak{b}_k}).
\end{aligned}
$$

Applying again the Associativity Formula, with the ideal $\mathfrak{d}$ and πJ interchanged, we obtain the equation

$$
\begin{aligned}
& e((\mathfrak{d},\pi,\mathfrak{p},\mathfrak{q}')J/(\mathfrak{p},\mathfrak{q}')J)\\
(2)\qquad & =\sum_{i,j,k,l} e((\pi,\mathfrak{p},\mathfrak{q}')J_{\mathfrak{c}_{ij,kl}}/(\mathfrak{p},\mathfrak{q}')J_{\mathfrak{c}_{ij,kl}})\cdot e((\mathfrak{d},\mathfrak{c}_{ij,kl})J/\mathfrak{c}_{ij,kl})\\
& =\sum_{i,k} e((\pi,\mathfrak{p})R_{\mathfrak{a}_i}/\mathfrak{p}R_{\mathfrak{a}_i})\cdot e((\pi,\mathfrak{q})R_{\mathfrak{b}_k}/\mathfrak{q}R_{\mathfrak{b}_k})\cdot\Big(\sum_{j,l} e((\mathfrak{d},\mathfrak{c}_{ij,kl})J/\mathfrak{c}_{ij,kl})\Big)\\
& =\sum_{i,k}\mu(\mathrm{A}_i,\bar{\mathfrak{X}})\cdot\mu(\mathrm{B}_k,\bar{\mathfrak{Y}})\cdot i(\alpha;\mathrm{A}_i\cdot\mathrm{B}_k)=i(\alpha;\bar{\mathfrak{X}}\cdot\bar{\mathfrak{Y}}).
\end{aligned}
$$

Combining the equations (1) and (2), we obtain the equation $\deg\mathfrak{Z}=i(\alpha;\bar{\mathfrak{X}}\cdot\bar{\mathfrak{Y}})$, which proves our assertion.

We can summarize our results in the following theorem:

THEOREM 4. *Let V^n be a variety in S^m, defined over a field K which is complete with respect to a real discrete valuation v, and let $\mathfrak{X}^r$ and $\mathfrak{Y}^s$ $(r+s=n)$ be two positive cycles in V, rational over K; let $\bar{V}$, $\bar{\mathfrak{X}}$, and $\bar{\mathfrak{Y}}$ be the specializations of V, $\mathfrak{X}$, and $\mathfrak{Y}$ respectively over v. If α is a rational point over $\bar{K}$ in $\bar{V}$ such that $\bar{V}$ is simple at α and that $\bar{\mathfrak{X}}$ and $\bar{\mathfrak{Y}}$ intersect properly at α, then there exists exactly one positive* 0-*cycle $\mathfrak{Z}$ in V, with support in $|\mathfrak{X}|\cap|\mathfrak{Y}|$, such that $\mathfrak{Z}$ is rational over K and its specialization $\bar{\mathfrak{Z}}$ over v consists of the point α with the coefficient $i(\alpha;\bar{\mathfrak{X}}\cdot\bar{\mathfrak{Y}})$; furthermore, a point a in $|\mathfrak{X}|\cap|\mathfrak{Y}|$ specializes to α over the specialization $(\mathfrak{X},\mathfrak{Y})\rightarrow(\bar{\mathfrak{X}},\bar{\mathfrak{Y}})$ if and only if $\mu(\alpha,\mathfrak{Z})>0$, and when such is the case, we have $i(a;\mathfrak{X}\cdot\mathfrak{Y})=\mu(a,\mathfrak{Z})$.*

THE JOHNS HOPKINS UNIVERSITY.

SPHERICAL FUNCTIONS ON A SEMISIMPLE LIE GROUP II.*

By Harish-Chandra.[1]

1. Introduction. Define G and K as in [2(i), § 1] and let $I_2(G)$ be the Hilbert space of all square-integrable spherical functions on G. Our main problem is to give an explicit "expansion" of a function f in $I_2(G)$, in terms of the elementary spherical functions. We shall construct a subspace $I_0(G)$ of $I_2(G)$ and give the required expansion for elements in $I_0(G)$. It seems likely that $I_0(G)$ is actually dense in $I_2(G)$. If this could be proved, our problem would be solved completely.

We have seen in [2(i), § 1] that a certain class of elementary spherical functions are parameterized by the space E/W. Fix a point λ in E. Then in [2(i)], we have studied the asymptotic behaviour of ϕ_λ on[2] $A_{\mathfrak{p}}$ at points which are far away from the singular[3] set. In this paper we shall consider the singular points as well. The main object here is to show that $\phi_\lambda(x)$ goes to zero very fast as x approaches infinity on G (see Theorem 2 of Section 12). Now let $d\lambda$ denote the Euclidean measure on E and put

$$\phi_a'(x) = \int_E \pi(\lambda) a(\lambda) \phi_\lambda(x)\, d\lambda \qquad (x \in G, a \in C_c^\infty(E)),$$

where π has the same meaning as in [2(i), § 3]. Let $I_0'(G)$ stand for the space of all such functions ϕ_a'. Then we shall prove that for $f \in I_0'(G)$, the integral

$$\bar{f}(\lambda) = \int_G f(x) \phi_\lambda(x^{-1})\, dx \qquad (\lambda \in E)$$

is well defined and, in fact, it is possible to normalize dx in such a way that[2]

$$\int_G |f(x)|^2\, dx = \int_E |\bar{f}(\lambda)|^2 |\mathbf{c}(\lambda)|^{-2}\, d\lambda$$

for all f in $I_0'(G)$. In order to extend this formula to functions on $I_2(G)$,

---

* Received July 16, 1957.

[1] John Simon Guggenheim fellow.

[2] As far as possible we keep to the notation of [2(i)]. Hence any symbol which is not explicitly defined afresh should be given the same meaning as in [2(i)].

[3] We recall that a point $h \in A_{\mathfrak{p}}$ is called singular if $\Delta(h) = 0$.

one would have to show that $I_0'(G)$ is dense in $I_2(G)$. This however still remains to be done.

The central idea of this paper can be described as follows. We give a method of reducing questions about spherical functions on G to similar questions on a proper subgroup of G. This process enables us to use induction. Again, it is the detailed consideration of certain differential equations on G, which permits us to effect this reduction. Since we are primarily interested in the asymptotic behaviour of the corresponding solutions, we have to undertake a study of the asymptotic behaviour of the coefficients of these equations. This is done in Sections 2 to 5. Lemma 17 and its corollary bring these equations into a manageable form and we then obtain (in Section 6) some rather rough estimates concerning the behaviour of the corresponding solutions at infinity. These, in turn, enable us to prove certain results on convergence in Sections 7 and 8 and to simplify the equations by replacing them by their asymptotic form (see Lemma 24). It is this step which brings about the reduction of the problem from G to a proper subgroup (see Lemmas 27, 30 and 35).

Now we combine the above reduction with induction and first use it to make a detailed study of the function $\boldsymbol{c}$ in Section 9. In particular, we show that $|\boldsymbol{c}(s\lambda)| = |\boldsymbol{c}(\lambda)|$ for $s \in W$ and $\boldsymbol{c}^{-1}$ is analytic on E. The same method is then applied in Sections 11 and 12 to study ϕ_λ and ϕ_a' ($\lambda \in E$, $a \in C_c^\infty(E)$). The main results are contained in Theorems 1, 2 and 3.

In Section 13 we show that the mapping $a \to \int \phi_a'(x)\phi_\lambda(x^{-1})\,dx$ ($a \in C_c^\infty(E)$), for a fixed $\lambda \in E$, is a distribution on E which is given by a simple formula (see the corollary of Lemma 41). However this formula involves an unknown coefficient $\boldsymbol{\beta}(\lambda)$ and the rest of the paper is devoted to establishing a relationship between $\boldsymbol{\beta}$ and $\boldsymbol{c}$. This requires a considerable amount of fresh work. First we prove an inequality (Lemma 42) in order to ensure the convergence of some integrals taken over a certain nilpotent subgroup $\bar{N}$ of G. The corollary of Lemma 43 expresses the value of these integrals in terms of the function $\boldsymbol{\beta}$. On the other hand we show in Section 15 (Theorem 4) that the same integrals can also be expressed by means of $\boldsymbol{c}$ and this gives the required connection between $\boldsymbol{\beta}$ and $\boldsymbol{c}$. However, the proof of Theorem 4 is rather long. It depends upon a detailed study of certain differential equations on the solvable group $\bar{N}A_{\mathfrak{p}}$.

Finally in Section 16, we state two conjectures and show how one can obtain an explicit Plancherel formula for spherical functions on G, by assuming their validity.

The principal results of this paper have been announced in a short note [2(k)].

2. The ring $\mathfrak{R}$. Define $\mathfrak{h}_{\mathfrak{p}_0}{}^+$ as in [2(i), § 9] and fix an element $H_0 \neq 0$ in[2] $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. Let $\mathfrak{m}_0$ be the centralizer of H_0 in $\mathfrak{g}_0$. Then if θ is the automorphism of $\mathfrak{g}$ given by $\theta(X+Y)=X-Y$ $(X \in \mathfrak{k}, Y \in \mathfrak{p})$, it is obvious that $\theta(\mathfrak{m}_0)=\mathfrak{m}_0$. This implies (see [2(h), Lemma 10]) that $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$. Let $\mathfrak{m}$ be the complexification of $\mathfrak{m}_0$ in $\mathfrak{g}$. We regard $\mathfrak{g}$ as a Hilbert space in the usual way [2(i), § 9] and consider the orthogonal complement $\mathfrak{q}$ of $\mathfrak{m}$ in $\mathfrak{g}$. Then $\theta(\mathfrak{q})=\mathfrak{q}$ and $[\mathfrak{m},\mathfrak{q}] \subset \mathfrak{q}$. Let $\mathfrak{l}$ be the centralizer of $\mathfrak{m}$ in $\mathfrak{h}_{\mathfrak{p}}$ and put $\mathfrak{l}_0=\mathfrak{l} \cap \mathfrak{h}_{\mathfrak{p}_0}$.

As before let P denote the set of all positive roots of $\mathfrak{g}$ (with respect to $\mathfrak{h}$). Then $\alpha(H_0) \geqq 0$ for $\alpha \in P$. Let Q be the set of those $\alpha \in P$ for which $\alpha(H_0)>0$. Put $\mathfrak{q}_+=\sum_{\alpha \in Q} CX_\alpha$, $\mathfrak{q}_-=\sum_{\alpha \in Q} CX_{-\alpha}$ where X_α has the usual meaning (see [2(i), § 7]). Then $\mathfrak{q}=\mathfrak{q}_+ + \mathfrak{q}_-$ and $\mathfrak{m}=\mathfrak{h}+\sum_{\alpha \in P'}(CX_\alpha + CX_{-\alpha})$, P' being the complement of Q in P. It is now obvious that $[\mathfrak{m},\mathfrak{q}_+] \subset \mathfrak{q}_+$, $[\mathfrak{m},\mathfrak{q}_-] \subset \mathfrak{q}_-$.

Let M and M_K be the analytic subgroups of G corresponding to $\mathfrak{m}_0$ and $\mathfrak{m}_{\mathfrak{k}_0}=\mathfrak{m}_0 \cap \mathfrak{k}_0$ respectively, Put $\mathfrak{m}_{\mathfrak{p}_0}=\mathfrak{m}_0 \cap \mathfrak{p}_0$ and let $M_{\mathfrak{p}}$ be the set of all elements in M of the form $\exp Y$ $(Y \in \mathfrak{m}_{\mathfrak{p}_0})$. Also put[4]

$$\Delta_M(m)=\det(\mathrm{Ad}(m)-\mathrm{Ad}(\theta(m)))_{\mathfrak{q}_+} \qquad (m \in M)$$

where the subscript denotes restriction on $\mathfrak{q}_+$. If $m=kp$ $(k \in M_K, p \in M_{\mathfrak{p}})$, it is obvious that $\Delta_M(m)=\det(\mathrm{Ad}(k))_{\mathfrak{q}_+}\Delta_M(p)$. Let M' be the set of those points $m \in M$ where $\Delta_M(m) \neq 0$. Then it follows that $M'=M_K M' M_K$ and $(M')^{-1}=M'$. Moreover

$$\Delta_M(\exp H)=\prod_{\alpha \in Q}(e^{\alpha(H)}-e^{-\alpha(H)}) \qquad (H \in \mathfrak{h}_{\mathfrak{p}_0}).$$

Let m be an element in M'. Since $\theta(\mathfrak{q}_+)=\mathfrak{q}_-$, it is clear that $X \to \{\mathrm{Ad}(m^{-1})-\mathrm{Ad}(\theta(m^{-1}))\}X$ $(X \in \mathfrak{q})$ is a nonsingular linear mapping of $\mathfrak{q}$. We denote its inverse by $A(m)$.

Lemma 1. *Put* $\mathfrak{q}_{\mathfrak{k}}=\mathfrak{q} \cap \mathfrak{k}$ *and* $\mathfrak{q}_{\mathfrak{p}}=\mathfrak{q} \cap \mathfrak{p}$. *Then if* $m \in M'$, $A(m)\mathfrak{q}_{\mathfrak{k}}=\mathfrak{q}_{\mathfrak{p}}$ *and* $A(m)\mathfrak{q}_{\mathfrak{p}}=\mathfrak{q}_{\mathfrak{k}}$.

Since $\theta(\mathrm{Ad}(x)Y)=\mathrm{Ad}(\theta(x))\theta(Y)$ $(x \in G, Y \in \mathfrak{g})$, it is obvious that under the mapping $\mathrm{Ad}(x)-\mathrm{Ad}(\theta(x))$, $\mathfrak{k}$ is mapped into $\mathfrak{p}$ and $\mathfrak{p}$ into $\mathfrak{k}$. From this our assertion follows immediately.

---

[4] Here we have extended θ to an automorphism of G.

For any $m \in M'$, define a linear transformation $c(m)$ on $\mathfrak{q}$ by $c(m)X = \mathrm{Ad}(m^{-1})A(m)X$ $(X \in \mathfrak{q})$. Then both $\mathfrak{q}_+$ and $\mathfrak{q}_-$ are invariant under $c(m)$. Let

$$c(m)X_\alpha = \sum_{\beta \in Q} X_\beta c_{\beta\alpha}(m) \qquad (\alpha \in Q,\ c_{\beta\alpha}(m) \in C).$$

Then $c_{\beta\alpha}(m)$, regarded as a function of m, is analytic on M'. Let $\mathfrak{R}_0$ be the ring of analytic functions on M' generated[5] over C by $c_{\beta\alpha}$ $(\beta, \alpha \in Q)$. Let $k \in M_K$ and $m \in M'$. Then it is easy to verify that $c(km) = c(m)$ and $c(mk)X = \mathrm{Ad}(k^{-1})c(m)\mathrm{Ad}(k)X$ $(X \in \mathfrak{q})$. Moreover

$$\begin{aligned}\theta(c(m)X) &= \mathrm{Ad}(\theta(m^{-1}))\theta(A(m)X) = -\mathrm{Ad}\,\theta(m^{-1})A(m)\theta(X)\\ &= \theta(X) - c(m)\theta(X),\end{aligned}$$

and therefore

$$\begin{aligned}c(m)\theta(X_\alpha) &= \theta(X_\alpha) - \theta(c(m)X_\alpha)\\ &= \theta(X_\alpha) - \sum_{\beta \in Q} \theta(X_\beta)c_{\beta\alpha}(m) \qquad (\alpha \in Q).\end{aligned}$$

Hence we get the following result.

LEMMA 2. *Let k be an element in M_K and g in $\mathfrak{R}_0$. Then $g(km) = g(m)$ $(m \in M')$ and the function $m \to g(mk)$ is also in $\mathfrak{R}_0$. Moreover the matrix coefficients of $c(m)$ (with respect to any fixed base of $\mathfrak{q}$), considered as functions on M', lie in the ring $C + \mathfrak{R}_0$.*

Now for any $x \in G$, put $x^\dagger = \theta(x^{-1})$.

LEMMA 3. $(1 - \mathrm{Ad}(m^\dagger m))c(m)X = X$ *for* $X \in \mathfrak{q}$ *and* $m \in M'$.

For $c(m)X = \mathrm{Ad}(m^{-1})A(m)X$ and therefore $(1 - \mathrm{Ad}(m^\dagger m))c(m)X = (\mathrm{Ad}(m^{-1}) - \mathrm{Ad}(m^\dagger))A(m)X = X$.

Let U be any linear subspace of $\mathfrak{g}$ containing $\mathfrak{q}_+$ and let T be a linear transformation in U which leaves $\mathfrak{q}_+$ invariant. Then we set $|T|_+ = \sup \|TX\|$ where X runs over all elements in $\mathfrak{q}_+$ with $\|X\| \leqq 1$. Let M_+ be the set of those points $m \in M$ where $|\mathrm{Ad}(m^{-1})|_+ < 1$. It is obvious that $M_+ \subset M'$, $A_{\mathfrak{p}}{}^+ \subset M_+$ and $M_K M_+ M_K = M_+$. Moreover if m_1, m_2 are in M_+, the same holds for $m_1 m_2$.

LEMMA 4. *Let m be an element in M_+. Then*

$$|c(m)|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^2 \{1 - |\mathrm{Ad}(m^{-1})|_+^2\}^{-1}.$$

---

[5] This means that $\mathfrak{R}_0$ consists of those functions on M' which can be written as polynomials in $c_{\beta\alpha}$ (with complex coefficients), the constant term of the polynomial being zero.

It is clear that $\mathrm{Ad}(m^{\dagger})$ is the adjoint of $\mathrm{Ad}(m)$ (in the sense of Hilbert space theory). Hence $|\mathrm{Ad}(m^{\dagger}m)^{-1}|_{+} \leqq |\mathrm{Ad}(m^{-1})|_{+}^{2} < 1$. Therefore since

$$(1 - \mathrm{Ad}((m^{\dagger}m)^{-1}))c(m)X = -\mathrm{Ad}((m^{\dagger}m)^{-1})X \qquad (X \in \mathfrak{q}_{+})$$

from Lemma 3, it is clear that

$$c(m)X = -\sum_{1 \leqq r < \infty} \mathrm{Ad}((m^{\dagger}m)^{-r})X.$$

Hence $|c(m)|_{+} \leqq \sum_{1 \leqq r < \infty} |\mathrm{Ad}(m^{-1})|_{+}^{2r} = |\mathrm{Ad}(m^{-1})|_{+}^{2}\{1 - |\mathrm{Ad}(m^{-1})|_{+}^{2}\}^{-1}$.

As usual let $\mathfrak{B}$ denote the universal enveloping algebra of $\mathfrak{g}$ and consider the subalgebra $\mathfrak{M}$ of $\mathfrak{B}$ generated by $(1, \mathfrak{m})$. We can regard any element μ of $\mathfrak{M}$ as a left-invariant differential operator on M. Applying this operator to each coefficient of the matrix of $c(m)$ (corresponding to some fixed base of $\mathfrak{q}$), we get a linear transformation $c(m;\mu)$ on $\mathfrak{q}$ $(m \in M')$.

LEMMA 5. *Let μ be any element in $\mathfrak{M}$ of degree r. Then there exists a positive number a such that*

$$|c(m;\mu)|_{+} \leqq a\,|\mathrm{Ad}(m^{-1})|_{+}^{2}\{1 - |\mathrm{Ad}(m^{-1})|_{+}^{2}\}^{-(r+1)}$$

for all $m \in M_{+}$.

Let σ denote the representation of $\mathfrak{M}$ on $\mathfrak{q}_{+}$ defined by $\sigma(Y)X = [Y, X]$ $(Y \in \mathfrak{m}, X \in \mathfrak{q}_{+})$. We shall first prove the following result.

LEMMA 6. *Let μ be an element in $\mathfrak{M}$ of degree r. Then we can select a finite number of elements $\mu_{ij} \in \mathfrak{M}$ $(1 \leqq i \leqq 5, 1 \leqq j \leqq s)$ with the following properties. μ_{3j} are of degree lower than r and*

$$\begin{aligned}(1 - \mathrm{Ad}(m^{\dagger}m)^{-1})c(m;\mu)X = &\sum_{1 \leqq j \leqq s} \sigma(\mu_{1j})\mathrm{Ad}((m^{\dagger}m)^{-1})\sigma(\mu_{2j})c(m;\mu_{3j})X \\ &+ \sum_{1 \leqq j \leqq s} \sigma(\mu_{4j})\mathrm{Ad}((m^{\dagger}m)^{-1})\sigma(\mu_{5j})X\end{aligned}$$

for all $X \in \mathfrak{q}_{+}$ and $m \in M'$.

If $r = 0$, our statement follows from Lemma 3. So now suppose $r \geqq 1$ and use induction. It is clearly enough to consider the case when $\mu = Y_1 Y_2 \cdots Y_r$ $(Y_i \in \mathfrak{m}_0)$. Put $\mu_0 = Y_2 \cdots Y_r$ and $m_t = m \exp tY_1$ for $m \in M$ and $t \in R$. Then if $X \in \mathfrak{q}_{+}$, $m \in M'$, it is obvious that

$$\begin{aligned}&[(d/dt)\{(1 - \mathrm{Ad}(m_t^{\dagger}m_t)^{-1})c(m_t;\mu_0)X\}]_{t=0} \\ &\quad = (1 - \mathrm{Ad}(m^{\dagger}m)^{-1})c(m;\mu)X + \sigma(Y_1)\mathrm{Ad}(m^{\dagger}m)^{-1}c(m;\mu_0)X \\ &\qquad - \mathrm{Ad}(m^{\dagger}m)^{-1}\sigma(\theta(Y_1))c(m;\mu_0)X.\end{aligned}$$

On the other hand our induction hypothesis is applicable to μ_0 and so we can choose elements $\nu_{ij} \in \mathfrak{M}$ $(1 \leqq i \leqq 5, 1 \leqq j \leqq q)$ such that the degree of ν_{3j} is lower than $r-1$ and

$$(1-\mathrm{Ad}(m^\dagger m)^{-1})c(m;\mu_0)X = \sum_{1 \leqq j \leqq q} \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;\nu_{3j})X + \sum_{1 \leqq j \leqq q} \sigma(\nu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{5j})X$$

for $m \in M'$ and $X \in \mathfrak{q}_+$. Therefore

$$\begin{aligned}&[(d/dt)\{(1-\mathrm{Ad}(m_t^\dagger m_t)^{-1})c(m_t;\mu_0)X]_{t=0}\\ &\quad = \sum_{1 \leqq j \leqq q} \{-\sigma(\nu_{1j}Y_1)\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;\nu_{3j})\\ &\qquad + \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\theta(Y_1)\nu_{2j})c(m;\nu_{3j})\\ &\qquad + \sigma(\nu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{2j})c(m;Y_1\nu_{3j}) - \sigma(\nu_{4j}Y_1)\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\nu_{5j})\\ &\qquad + \sigma(\nu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\theta(Y_1)\nu_{5j})\}X.\end{aligned}$$

By equating the two expressions for

$$[(d/dt)\{(1-\mathrm{Ad}(m_t^\dagger m_t)^{-1})c(m_t;\mu_0)X\}]_{t=0}$$

obtained above, the assertion of the lemma follows.

Now we come to the proof of Lemma 6. If $r=0$, our statement is true in consequence of Lemma 4. Hence we may suppose that $r \geqq 1$ and use induction on r. But we know from Lemma 6 that

$$c(m;\mu)X = \sum_{1 \leqq j \leqq s} \sum_{0 \leqq k < \infty} \mathrm{Ad}(m^\dagger m)^{-k}\{\sigma(\mu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{2j})c(m;\mu_{3j})X + \sigma(\mu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{5j})X\}$$

for $X \in \mathfrak{q}_+$ and $m \in M_+$. Moreover

$$|\mathrm{Ad}(m^\dagger m)^{-k}\sigma(\mu_{1j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{2j})c(m;\mu_{3j})|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^{2(k+1)}\,|\sigma(\mu_{1j})|_+\,|\sigma(\mu_{2j})|_+\,|c(m;\mu_{3j})|_+$$

and the degree of μ_{3j} is less than r. Therefore if we apply the induction hypothesis to μ_{3j} and observe that

$$|\mathrm{Ad}(m^\dagger m)^{-k}\sigma(\mu_{4j})\mathrm{Ad}(m^\dagger m)^{-1}\sigma(\mu_{5j})|_+ \leqq |\mathrm{Ad}(m^{-1})|_+^{2(k+1)}\,|\sigma(\mu_{4j})|_+\,|\sigma(\mu_{5j})|_+,$$

the required result follows immediately.

Let $\mathfrak{R}$ be the ring of analytic functions on M' generated over C by all functions of the form $\mu c_{\alpha\beta}$ $(\mu \in \mathfrak{M}; \alpha, \beta \in Q)$. It is obvious that if $g \in \mathfrak{R}$ and $\mu \in \mathfrak{M}$, then μg is also in $\mathfrak{R}$. The following result is an immediate consequence of Lemma 5.

LEMMA 7. *Let g be an element in $\mathfrak{N}$. Then there exists a positive number a and an integer $r \geqq 1$ such that*

$$|g(m)| \leqq a\,|\mathrm{Ad}(m^{-1})|_+^2\{1 - |\mathrm{Ad}(m^{-1})|_+^2\}^{-r}$$

for all $m \in M_+$

3. The mapping μ_0. Let q be the number of roots in Q. Since $\mathfrak{g}$ is the orthogonal sum of $\mathfrak{m}$ and $\mathfrak{q}$, $\dim \mathfrak{g} = \dim \mathfrak{m} + \dim \mathfrak{q} = \dim \mathfrak{m} + 2q$. On the other hand, the restriction of $\mathrm{ad}\, H_0$ on $\mathfrak{q}$ is obviously nonsingular and therefore it defines a linear isomorphism of $\mathfrak{q}_\mathfrak{k}$ onto $\mathfrak{q}_\mathfrak{p}$. Hence $\dim \mathfrak{q}_\mathfrak{k} = \frac{1}{2} \dim \mathfrak{q} = q$. Let $X_\alpha = Y_\alpha + Z_\alpha$ $(Y_\alpha \in \mathfrak{p}, Z_\alpha \in \mathfrak{k})$ for $\alpha \in P$. Then $\theta(X_\alpha) = -Y_\alpha + Z_\alpha$. Since $X_\alpha, \theta(X_\alpha)$ $(\alpha \in Q)$ span $\mathfrak{q}$, it follows that Z_α $(\alpha \in Q)$ span $\mathfrak{q}_\mathfrak{k}$. Therefore Z_α $(\alpha \in Q)$ must be linearly independent over C. Put $\mathfrak{m}_\mathfrak{k} = \mathfrak{m} \cap \mathfrak{k}$ and $\mathfrak{m}_\mathfrak{p} = \mathfrak{m} \cap \mathfrak{p}$.

LEMMA[6] 8. *Suppose m is an element in M'. Then $\mathfrak{g} = \mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} + \mathfrak{m}_\mathfrak{p} + \mathfrak{k}$ where the sum is direct.*

Since $\mathfrak{m}_\mathfrak{p} + \mathfrak{k} = \mathfrak{m} + \mathfrak{q}_\mathfrak{k}$ and $\dim \mathfrak{g} = \dim \mathfrak{m} + 2 \dim \mathfrak{q}_\mathfrak{k}$, it would be enough to prove that $\mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} \cap (\mathfrak{m}_\mathfrak{p} + \mathfrak{k}) = \{0\}$. So let us suppose that $X \in \mathfrak{q}_\mathfrak{k}$ and $\mathrm{Ad}(m^{-1})X \in \mathfrak{m}_\mathfrak{p} + \mathfrak{k}$. Then $(\mathrm{ad}\, H_0)^2 \mathrm{Ad}(m^{-1})X \in \mathfrak{k}$ and therefore

$$(\mathrm{ad}\, H_0)^2 \mathrm{Ad}(m^{-1})\, X = \theta((\mathrm{ad}\, H_0)^2 \mathrm{Ad}(m^{-1})X) = (\mathrm{ad}\, H_0)^2 \mathrm{Ad}(m^\dagger)X.$$

This shows that $(\mathrm{ad}\, H_0)^2(\mathrm{Ad}\, m^{-1} - \mathrm{Ad}\, m^\dagger)X = 0$. But since $\mathrm{ad}\, H_0$ defines a nonsingular linear transformation on $\mathfrak{q}$ and since $m \in M'$, it is now clear that $X = 0$. This proves that $\mathrm{Ad}(m^{-1})\mathfrak{q}_\mathfrak{k} \cap (\mathfrak{m}_\mathfrak{p} + \mathfrak{k}) = \{0\}$.

Let $\mathfrak{X}$ be the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{k})$ and let $\mathfrak{Q}_\mathfrak{k}$ and $\mathfrak{M}_\mathfrak{p}$ be the images in $\mathfrak{B}$ of[7] $S(\mathfrak{q}_\mathfrak{k})$ and $S(\mathfrak{m}_\mathfrak{p})$ respectively under the canonical mapping (see [2(b), p. 192]) of $S(\mathfrak{g})$ into $\mathfrak{B}$. Moreover for any $x \in G$, let $b \rightarrow b^x$ $(b \in \mathfrak{B})$ denote the automorphism of $\mathfrak{B}$ which coincides with $\mathrm{Ad}(x)$ on $\mathfrak{g}$. Consider the tensor product $V = \mathfrak{Q}_\mathfrak{k} \times \mathfrak{M}_\mathfrak{p} \times \mathfrak{X}$. Then it follows from the above result and Lemma 12 of [2(b)] that for any $m \in M'$, there exists a linear isomorphism of V onto $\mathfrak{B}$ which maps $q \times \mu \times x$ on $q^{m^{-1}}\mu x$ $(q \in \mathfrak{Q}_\mathfrak{k}, \mu \in \mathfrak{M}_\mathfrak{p}, x \in \mathfrak{X})$. Hence $\mathfrak{B} = (\mathfrak{Q}_\mathfrak{k})^{m^{-1}}\mathfrak{M}_\mathfrak{p}\mathfrak{X}$. Let $\mathfrak{Q}_\mathfrak{k}'$ denote the subspace consisting of those elements in $\mathfrak{Q}_\mathfrak{k}$ whose homogeneous component (see [2(i), Footnote 21]) of degree zero is zero. Then since V is the direct sum of $\mathfrak{Q}_\mathfrak{k} \times \mathfrak{M}_\mathfrak{p} \times (\mathfrak{X}\mathfrak{k})$, $\mathfrak{Q}_\mathfrak{k}' \times \mathfrak{M}_\mathfrak{p} \times 1$ and $1 \times \mathfrak{M}_\mathfrak{p} \times 1$, the following corollary is obvious.

---

[6] Cf. [2(i), Lemma 21].

[7] Here we follow the notation introduced in [2(g), § 2].

COROLLARY. *Suppose m lies in M'. Then*

$$\mathfrak{B} = (\mathfrak{Q}_{\mathfrak{k}})^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}\mathfrak{X} = \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}} + \mathfrak{M}_{\mathfrak{p}}$$

where the sum is direct.

For any finite set of elements $X_1, \cdots, X_d \in \mathfrak{g}$, put

$$\sigma(X_1, X_2, \cdots, X_d) = (d\,!)^{-1} \sum X_{i_1} X_{i_2} \cdots X_{i_d} \in \mathfrak{B},$$

where the sum is over all permutations $(i_1, \cdots, i_d)$ of $(1, 2, \cdots, d)$. Moreover let $\mathfrak{B}_d$ denote the set of all element in $\mathfrak{B}$ of degree $\leqq d$.

LEMMA 9. *Let b be a given element in $\mathfrak{B}_d$. Then we can choose μ_0 in $\mathfrak{M}_{\mathfrak{p}} \cap \mathfrak{B}_d$ and a finite number of elements $\mu_i \in \mathfrak{M}_{\mathfrak{p}} \cap \mathfrak{B}_{d-1}$, $g_i \in \mathfrak{R}_0$ $(1 \leqq i \leqq r)$ such that*

$$b - \mu_0 - \sum_{1 \leqq i \leqq r} g_i(m)\mu_i \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}$$

for all $m \in M'$.

We shall use the induction on d. Since $\mathfrak{g} = \mathfrak{q}_{\mathfrak{p}} + \mathfrak{m}_{\mathfrak{p}} + \mathfrak{k}$, it is obviously enough to consider the case when $b = \sigma(Y_1, \cdots, Y_e)\mu$ and $Y_j \in \mathfrak{q}_{\mathfrak{p}}$, $\mu \in \mathfrak{M}_{\mathfrak{p}}$ and μ is of degree $d - e$ $(e \geqq 1)$. Now for any $Y \in \mathfrak{q}_{\mathfrak{p}}$ and $m \in M'$,

$$c(m)Y = \operatorname{Ad}(m^{-1})A(m)Y = \tfrac{1}{2}Y + \tfrac{1}{2}(\operatorname{Ad}(m^{-1}) + \operatorname{Ad}\theta(m^{-1}))A(m)Y.$$

Since $A(m)Y \in \mathfrak{q}_{\mathfrak{k}} \subset \mathfrak{k}$ from Lemma 1, it is clear that $c(m)Y - \tfrac{1}{2}Y \in \mathfrak{k}$. Put

$$U_i(m) = 2A(m)Y_i, \qquad V_i(m) = 2c(m)Y_i - Y_i \qquad (1 \leqq i \leqq e).$$

Then $U_i(m)$, $V_i(m)$ are in $\mathfrak{k}$ and $\operatorname{Ad}(m^{-1})U_i(m) = Y_i + V_i(m)$. Let $(i_1, i_2, \cdots, i_e)$ be any permutation of $(1, 2, \cdots, e)$. Then

$$\begin{aligned}(U_{i_1}(m) \cdots U_{i_e}(m))^{m^{-1}}\mu &= (Y_{i_1} + V_{i_1}(m)) \cdots (Y_{i_e} + V_{i_e}(m))\mu \\ &= (L_{i_1} + R_{i_1} - D_{i_1}) \cdots (L_{i_e} + R_{i_e} - D_{i_e})\mu \\ &\equiv (L_{i_1} - D_{i_1}) \cdots (L_{i_e} - D_{i_e})\mu \bmod \mathfrak{B}\mathfrak{k}.\end{aligned}$$

Here L_i, R_i and D_i respectively denote the linear mappings $a \rightarrow Y_i a$, $a \rightarrow aV_i(m)$ and $a \rightarrow [V_i(m), a] = V_i(m)a - aV_i(m)$ $(a \in \mathfrak{B})$ of $\mathfrak{B}$ into itself. Since $[X, a] \in \mathfrak{B}_r$ for $X \in \mathfrak{g}$ and $a \in \mathfrak{B}_r$, it follows from Lemma 2 that we can select $b_1, \cdots, b_s \in \mathfrak{B}_{d-1}$ and $g_1', \cdots, g_s' \in C + \mathfrak{R}_0$ such that

$$(\sigma(U_1(m), \cdots, U_e(m))^{m^{-1}}\mu \equiv b + \sum_{1 \leqq i \leqq s} g_i'(m) b_i \bmod \mathfrak{B}\mathfrak{k}$$

for all $m \in M'$. But $\sigma(U_1(m), \cdots, U_e(m)) \in \mathfrak{Q}_{\mathfrak{k}}'$ since $U_j(m) \in \mathfrak{q}_{\mathfrak{k}}$ and therefore

$$b \equiv -\sum_{1 \leqq i \leqq s} g_i'(m) b_i \bmod \{\mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}\}.$$

Our assertion now follows immediately by the induction hypothesis.

Let $\mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}}$ denote the set of all differential operators on M' which are of the form $\sum_{1 \leqq i \leqq r} g_i\mu_i$ $(g_i \in \mathfrak{R}_0, \mu_i \in \mathfrak{M}_{\mathfrak{p}})$. Then the above lemma shows that for any $b \in \mathfrak{B}$, we can select $\mu_0 \in \mathfrak{M}_{\mathfrak{p}}$ and $\mu \in \mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}}$, such that

$$b - \mu_0 - \mu_m \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}$$

for all $m \in M'$. (Here μ_m denotes, as usual, the local expression [2(d), p. 112] of μ at m.) Moreover it follows from the Corollary of Lemma 8 that the differential operator $\mu_0 + \mu$ on M' is uniquely determined by b. Now suppose $\mu_0 + \mu = \mu_0' + \mu'$ $(\mu_0' \in \mathfrak{M}_{\mathfrak{p}}, \mu' \in \mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}})$. Then $\mu_0 - \mu_0' = \mu' - \mu$ and therefore $\mu_0 - \mu_0' = (\mu' - \mu)_m$ for every $m \in M'$. In particular we can take $m = \exp tH_0$ $(t > 0)$. Then if $g \in \mathfrak{R}_0$, it follows from Lemma 7 that $\lim_{t \to +\infty} g(\exp tH_0) = 0$. Therefore $\mu_0 - \mu_0' = 0$. This proves that both μ_0 and μ are uniquely determined by b. We shall denote them by $\mu_0(b)$ and $\mu(b)$ respectively.

Lemma 10. *Let k be an element in M_K. Then $(\mu_0(b))^k = \mu_0(b^k)$ and*[8] *$\mu(b)^k = \mu(b^k)$ for $b \in \mathfrak{B}$.*

Since $b - \mu_0(b) - \mu_m(b) \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}$ $(m \in M')$, it follows that

$$b^k - \mu_0(b)^k - (\mu_m(b))^k \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{km^{-1}}\mathfrak{M}_{\mathfrak{p}}.$$

Therefore replacing m by mk, we find that

$$b^k - \mu_0(b)^k - (\mu_{mk}(b))^k \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}.$$

Now $(\mu(b)^k)_m = (\mu(b)_{k^{-1}mk})^k$ from Lemma 14 of [2(d)]. But it is clear from Lemma 2 that the differential operator $\mu(b)^k$ lies in $\mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}}$ and $\mu(b)_{k^{-1}mk} = \mu(b)_{mk}$. Therefore

$$b^k - \mu_0(b)^k - (\mu(b)^k)_m \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_{\mathfrak{k}}')^{m^{-1}}\mathfrak{M}_{\mathfrak{p}}$$

and this proves that $\mu_0(b^k) = \mu_0(b)^k$ and $\mu(b^k) = \mu(b)^k$.

Let $I_{\mathfrak{g}}$ be the centralizer of $\mathfrak{k}$ in $\mathfrak{B}$ and $I_{\mathfrak{m}}$ the centralizer of $\mathfrak{m}_{\mathfrak{k}}$ in $\mathfrak{M}$.

Corollary. *If $b \in I_{\mathfrak{g}}$ then $\mu_0(b) \in I_{\mathfrak{m}}$.*

This is obvious from Lemma 10.

---

[8] See [2(d), p. 118] for the definition of $\mu(b)^k$.

For any $b \in \mathfrak{B}$, define the differential operator $\delta'(b)$ on[2] $A_\mathfrak{p}'$ as in [2(i), § 5]. It is obvious that $A_\mathfrak{p}' \subset M'$.

LEMMA 11. *Let* b *be an element in* $\mathfrak{B}$ *and select* $g_i \in \mathfrak{R}_0, \mu_i \in \mathfrak{M}_\mathfrak{p}$ $(1 \leqq i \leqq r)$ *such that*

$$b - \mu_0(b) - \sum_{1 \leqq i \leqq r} g_i(m)\mu_i \in \mathfrak{B}\mathfrak{k} + (\mathfrak{Q}_\mathfrak{k}')^{m^{-1}}\mathfrak{M}_\mathfrak{p}$$

for all $m \in M'$. *Then*

$$\delta_h'(b) = \delta_h'(\mu_0(b)) + \sum_{1 \leqq i \leqq r} g_i(h)\delta_h'(\mu_i)$$

for $h \in A_\mathfrak{p}'$.

Clearly $\mathfrak{Q}_\mathfrak{k}' \subset \mathfrak{k}\mathfrak{B}$ and therefore

$$b - \mu_0(b) - \sum_{1 \leqq i \leqq r} g_i(h)\mu_i \in \mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h^{-1}}\mathfrak{B} \qquad (h \in A_\mathfrak{p}').$$

Also $a - \delta_h'(a) \in \mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h^{-1}}\mathfrak{B}$ for any $a \in \mathfrak{B}$. Therefore[2]

$$\delta_h'(b) - \delta_h'(\mu_0(b)) - \sum_{1 \leqq i \leqq r} g_i(h)\delta_h'(\mu_i) \in \{\mathfrak{B}\mathfrak{k} + \mathfrak{k}^{h^{-1}}\mathfrak{B}\} \cap \mathfrak{H}_\mathfrak{p} = \{0\}$$

from Corollary 2 to Lemma 21 of [2(i)].

4. The connection between μ_0 and γ. Define the homomorphism γ of $I_\mathfrak{g}$ onto $I(\mathfrak{h}_\mathfrak{p})$ as in Theorem 1 of [2(i)] and consider the subgroup W' consisting of those elements[2] $s \in W$ which leave H_0 fixed. Now $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$ and $\mathfrak{h}_{\mathfrak{p}_0}$ is a maximal abelian subspace of $\mathfrak{m}_{\mathfrak{p}_0}$. Therefore since $\mathfrak{m}_0$ is the centralizer of H_0 in $\mathfrak{g}_0$, it is clear that W' can also be considered as the little Weyl group[9] of $\mathfrak{m}_0$ with respect to $\mathfrak{h}_{\mathfrak{p}_0}$. Let J' be the ring of those elements in $\mathfrak{H}_\mathfrak{p}$ which are invariant under W'. Then corresponding to Theorem 1 of [2(i)], we have a homomorphism $\gamma_\mathfrak{m}$ of $I_\mathfrak{m}$ onto J'. Define the linear function σ on $\mathfrak{h}_\mathfrak{p}$ by $\sigma(H) = \frac{1}{2} \sum_{\beta \in P'} \beta(H)$ where P' is the subset of those roots in P which vanish at H_0.

LEMMA 12. $\gamma(q) = e^{\rho-\sigma}\gamma_\mathfrak{m}(\mu_0(q)) \circ e^{-(\rho-\sigma)}$ *for* $q \in I_\mathfrak{g}$.

Define $\delta(b)$ $(b \in \mathfrak{B})$ as in Lemma 26 of [2(i)]. Then it follows from Lemma 11 that $\delta_h(q) = \delta_h(\mu_0(q)) + \delta_h(\mu_h(q))$ for $h \in A_\mathfrak{p}'$. On the other hand

$$\delta(\mu_0(q)) = e^{\rho}\delta'(\mu_0(q)) \circ e^{-\rho} = e^{\rho-\sigma}\{e^{\sigma}\delta'(\mu_0(q)) \circ e^{-\sigma}\} \circ e^{-\rho+\sigma}.$$

Now put $h_t = \exp tH$ $(t \in R)$ where H is some fixed element in $\mathfrak{h}_{\mathfrak{p}_0}{}^+$. Then

---

[9] Here we are extending the notion of the little Weyl group [2(i), § 3] to reductive Lie algebras in the obvious way (see [2(d), p. 118]).

$h_t \in A_\mathfrak{p}'$ if $t > 0$. Hence if d is the degree of $\mathfrak{q}$ it follows from Lemma 26 of [2(i)] by taking limits in the finite-dimensional space $\mathfrak{B}_d$, that

$$\operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(q) = \gamma(q), \qquad \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_{h_t}(q)) = 0.$$

(Here we have to make use of Lemma 7 and the definition of $\mu(q)$.) Therefore $\gamma(q) = \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_0(q))$. On the other hand we can apply Corollary 2 to Lemma 21 of [2(i)] to $\mathfrak{m}$ instead of $\mathfrak{g}$. Hence for any $b \in \mathfrak{M}$ and $h \in A_\mathfrak{p}'$, there exists a unique element u in $\mathfrak{H}_\mathfrak{p}$ such that $b - u \in (\mathfrak{m}_\mathfrak{k})^{h^{-1}}\mathfrak{M} + \mathfrak{M}\mathfrak{m}_\mathfrak{k}$. But then it follows from the definition of $\delta'(b)$ that $u = \delta_h'(b)$. Now put $\delta''(b) = e^{\sigma}\delta'(b) \circ e^{-\sigma}$ and apply Lemma 26 of [2(i)] to $\mathfrak{m}$. Then it follows that $\operatorname*{Lim}_{t\to+\infty} \delta_{h_t}''(b) = \gamma_\mathfrak{m}(b)$ provided $b \in I_\mathfrak{m}$. By the Corollary of Lemma 10, this holds in particular if $b = \mu_0(q)$. But since

$$\delta(\mu_0(q)) = e^{\rho-\sigma}\delta''(\mu_0(q)) \circ e^{-\rho+\sigma},$$

it is obvious that

$$\gamma(q) = \operatorname*{Lim}_{t\to+\infty} \delta_{h_t}(\mu_0(q)) = e^{\rho-\sigma}\gamma_\mathfrak{m}(\mu_0(q)) \circ e^{-\rho+\sigma}.$$

This proves the lemma.

COROLLARY. *Suppose* q_1, q_2 *are two elements in* $I_\mathfrak{g}$. *Then*

$$\mu_0(q_1)\mu_0(q_2) \equiv \mu_0(q_2)\mu_0(q_1) \equiv \mu_0(q_1q_2) \bmod \mathfrak{M}\mathfrak{m}_\mathfrak{k}.$$

Since $\gamma(q_1q_2) = \gamma(q_1)\gamma(q_2)$, it follows from Lemma 12 that $\gamma_\mathfrak{m}$ maps $\mu_0(q_1)\mu_0(q_2)$, $\mu_0(q_2)\mu_0(q_1)$ and $\mu_0(q_1q_2)$ into the same element $\gamma(q_1)\gamma(q_2)$. The required result now follows from the fact that the kernel of $\gamma_\mathfrak{m}$ is contained in $\mathfrak{M}\mathfrak{m}_\mathfrak{k}$ (see [2(i), Theorem 1]).

5. Some consequences of Lemma 12. For any linear function λ on $\mathfrak{h}_\mathfrak{p}$, let H_λ denote the corresponding element in $\mathfrak{h}_\mathfrak{p}$ so that $\langle H, H_\lambda\rangle = \lambda(H)$ for all $H \in \mathfrak{h}_\mathfrak{p}$. Also define $\mathfrak{I}$ and $\mathfrak{I}_0$ as in the beginning of Section 2.

LEMMA 13. $\rho - \sigma$ *is invariant under* W' *and* $H_{\rho-\sigma} \in \mathfrak{I}_0$.

Let $(\operatorname{ad} H)_{\mathfrak{q}_+}$ denote the restriction of $\operatorname{ad} H$ on $\mathfrak{q}_+$ for $H \in \mathfrak{h}_\mathfrak{p}$. It is obvious that $\operatorname{sp}(\operatorname{ad} H)_{\mathfrak{q}_+} = \rho(H) - \sigma(H)$. Since W' is the little Weyl group of $\mathfrak{m}$, we can, for any given $s \in W'$, choose $k \in M_K$ such that $\operatorname{Ad}(k)H = sH$. Since $\mathfrak{q}_+$ is invariant under k, it follows that $\operatorname{sp}(\operatorname{ad} H)_{\mathfrak{q}_+} = \operatorname{sp}(\operatorname{ad}(sH))_{\mathfrak{q}_+}$ and this shows that $\rho - \sigma$ is invariant under W'. Now in order to prove that $H_{\rho-\sigma} \in \mathfrak{I}_0$, it is obviously sufficient to verify that $\beta(H_{\rho-\sigma}) = 0$ for any root $\beta \in P$ for which $\beta(H_0) = 0$. Let α denote the restriction of β on $\mathfrak{h}_\mathfrak{p}$. We may assume that $\alpha \neq 0$. Consider the corresponding reflexion $s_\alpha \in W$ (see [2(i), § 3]). It is obvious that s_α lies in W' and therefore it must leave $H_{\rho-\sigma}$ fixed. Hence $\beta(H_{\rho-\sigma}) = \alpha(H_{\rho-\sigma}) = 0$.

Let ω denote the Casimir operator of $\mathfrak{g}$ (see [2(i), § 7]). We wish to compute $\mu_0(\omega)$.

LEMMA 14. *Let $X_1, \cdots, X_q$ be an orthonormal base for $\mathfrak{m}_{\mathfrak{p}_0}$ over R. Then $\mu_0(\omega) = X_1^2 + \cdots + X_q^2 + 2H_{\rho-\sigma}$.*

Put $\eta_0 = X_1^2 + \cdots + X_q^2$. It is easy to check that $\eta_0 \in I_\mathfrak{m}$ and if we apply Corollary 2 of Lemma 27 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$), it follows that $\gamma_\mathfrak{m}(\eta_0) = \bar{\omega} - \langle\sigma, \sigma\rangle$. However it is obvious that

$$e^{-\rho+\sigma}\bar{\omega} \circ e^{\rho-\sigma} = \bar{\omega} + 2H_{\rho-\sigma} + \langle\rho - \sigma, \rho - \sigma\rangle.$$

Therefore if $\eta = \eta_0 + 2H_{\rho-\sigma} - 2\langle\rho - \sigma, \sigma\rangle$, it follows again by the same corollary that

$$e^{\rho-\sigma}\gamma_\mathfrak{m}(\eta) \circ e^{-\rho+\sigma} = \bar{\omega} - \langle\rho, \rho\rangle = \gamma(\omega).$$

But in view of Lemma 12, this implies that $\gamma_\mathfrak{m}(\eta - \mu_0(\omega)) = 0$. However $\eta - \mu_0(\omega)$ lies in $\mathfrak{M}\mathfrak{k}_\mathfrak{p} \cap I_\mathfrak{m}$. Therefore it follows from [2(i), Lemma 19] that $\eta = \mu_0(\omega)$. But we have seen above that $\beta(H_{\rho-\sigma}) = 0$ if $\beta(H_0) = 0$ $(\beta \in P)$. Therefore $\langle\rho - \sigma, \sigma\rangle = 0$ and this proves our assertion.

Put $\gamma_\mathfrak{m}'(\nu) = e^{\rho-\sigma}\gamma_\mathfrak{m}(\nu) \circ e^{-\rho+\sigma}$ $(\nu \in I_\mathfrak{m})$. Since $\rho - \sigma$ is invariant under W', it is clear that $J' = \gamma_\mathfrak{m}(I_\mathfrak{m}) = \gamma_\mathfrak{m}'(I_\mathfrak{m})$. Put $r = [W : W']$ and choose elements $\nu_1 = 1, \nu_2, \cdots, \nu_r$ in $I_\mathfrak{m}$ such that $\gamma_\mathfrak{m}'(\nu_i)$ $(1 \leqq i \leqq r)$ are homogeneous and[2] $J' = \sum_{1 \leqq i \leqq r} J\gamma_\mathfrak{m}'(\nu_i)$. From Lemma 8 of [2(i)] this is possible.

LEMMA 15. $I_\mathfrak{m} \subset \sum_{1 \leqq i \leqq r} \nu_i\mu_0(I_\mathfrak{g}) + \mathfrak{M}\mathfrak{m}_\mathfrak{k}$.

Let ν be a given element in $I_\mathfrak{m}$. Then $\gamma_\mathfrak{m}'(\nu) \in J'$ and therefore $\gamma_\mathfrak{m}'(\nu) = \sum_{1 \leqq i \leqq r} \gamma(q_i)\gamma_\mathfrak{m}'(\nu_i)$ for suitable $q_i \in I_\mathfrak{g}$ since $\gamma(I_\mathfrak{g}) = J$. But $\gamma(q_i) = \gamma_\mathfrak{m}'(\mu_0(q_i))$ from Lemma 12 and therefore $\gamma_\mathfrak{m}'(\nu - \sum_{1 \leqq i \leqq r} \nu_i\mu_0(q_i)) = 0$. However the kernels of $\gamma_\mathfrak{m}$ and $\gamma_\mathfrak{m}'$ are the same and so by applying Theorem 1 of [2(i)] to $\mathfrak{m}$, we conclude that $\nu - \sum_i \nu_i\mu_0(q_i) \in \mathfrak{M}\mathfrak{m}_\mathfrak{k}$. This proves the lemma.

COROLLARY. *Suppose $\sum_{1 \leqq i \leqq r} \nu_i\mu_0(q_i) \in \mathfrak{M}\mathfrak{m}_\mathfrak{k}$ for some $q_i \in I_\mathfrak{g}$. Then $q_i \in \mathfrak{B}\mathfrak{k}$ $1 \leqq i \leqq r$.*

Put $\nu = \sum_i \nu_i\mu_0(q_i)$. Then $\nu \in I_\mathfrak{m} \cap (\mathfrak{M}\mathfrak{m}_\mathfrak{k})$ and therefore $\gamma_\mathfrak{m}(\nu) = 0$.

This implies that $\gamma_{\mathfrak{m}}'(v) = \sum_i \gamma_{\mathfrak{m}}'(\nu_i)\gamma(q_i) = 0$. But $\gamma_{\mathfrak{m}}'(\nu_i)$ $1 \leqq i \leqq r$ are linearly independent over $C(J)$ (see [2(i), Lemma 8]) and therefore $\gamma(q_i) = 0$ $1 \leqq i \leqq r$. Our assertion now follows from Theorem 1 of [2(i)].

The following lemma contains the main result of this section.

LEMMA 16. *Let ν be an element in $I_{\mathfrak{m}}$ and suppose $\nu - \sum_{1\leqq i\leqq r} \nu_i\mu_0(q_i) \in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$ $(q_i \in I_{\mathfrak{g}})$. Then we can select a finite number of elements $g_j \in \mathfrak{R}$ and $\tau_j \in \mathfrak{M}$ $(1 \leqq j \leqq s)$ with the following property. If ϕ is any spherical function on G of class C^∞,*

$$\phi(m;\nu) = \sum_{1\leqq i\leqq r} \phi(m;\nu_i q_i) + \sum_{1\leqq j\leqq s} g_j(m)\phi(m;\tau_j)$$

for all $m \in M'$.

It is obvious that $\phi(m;v) = 0$ for $v \in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$. Therefore $\phi(m;\nu) = \sum_i \phi(m;\nu_i\mu_0(q_i))$. On the other hand since

$$q_i - \mu_0(q_i) - \mu_m(q_i) \in \mathfrak{B}\mathfrak{k} + (\mathfrak{L}_{\mathfrak{l}}')^{m-1}\mathfrak{M}_{\mathfrak{p}},$$

it is clear that

$$\phi(m;\mu_0(q_i)) = \phi(m;q_i) - \phi(m;\mu(q_i)) \qquad (m \in M').$$

Therefore

$$\phi(m;\nu_i\mu_0(q_i)) = \phi(m;\nu_i q_i) - \phi(m;\nu_i \circ \mu(q_i))$$

and

$$\phi(m;\nu) = \sum_{1\leqq i\leqq r} \phi(m;\nu_i q_i) - \sum_{1\leqq i\leqq r} \phi(m;\nu_i \circ \mu(q_i)).$$

But since $\mu(q_i) \in \mathfrak{R}_0\mathfrak{M}_{\mathfrak{p}}$, it is obvious that $\sum_i \nu_i \circ \mu(q_i) = -\sum_{1\leqq j\leqq s} g_j\tau_j$ for suitable $g_j \in \mathfrak{R}$ and $\tau_j \in \mathfrak{M}$. This proves our assertion.

Let $l_0 = \dim \mathfrak{l}$ and let $\mathfrak{l}_0^+$ denote the set of those elements $H \in \mathfrak{l}_0$ for which $\alpha(H) > 0$ for every $\alpha \in Q$ (see Section 2 for the definition of Q). Then $H_0 \in \mathfrak{l}_0^+$. Select a base H_p $(1 \leqq p \leqq l_0)$ for $\mathfrak{l}_0$ over R and choose $q_{ijp} \in I_{\mathfrak{g}}$ $(1 \leqq i, j \leqq r, 1 \leqq p \leqq l_0)$ such that

$$H_p\nu_j \equiv \sum_{1\leqq i\leqq r} \nu_i\mu_0(q_{ijp}) \bmod \mathfrak{M}\mathfrak{m}_{\mathfrak{k}} \qquad (1 \leqq j \leqq r, 1 \leqq p \leqq l_0).$$

Then q_{ijp} are unique mod $(I_{\mathfrak{g}} \cap \mathfrak{B}\mathfrak{k})$ from the Corollary to Lemma 15. Moreover

$$H_sH_p\nu_j \equiv \sum_{1\leqq i\leqq r} H_s\nu_i\mu_0(q_{ijp}) \equiv \sum_{1\leqq i,k\leqq r} \nu_k\mu_0(q_{kis})\mu_0(q_{ijp}) \bmod \mathfrak{M}\mathfrak{m}_{\mathfrak{k}},$$

since $\mu_0(q_{ijp}) \in I_{\mathfrak{m}}$. But $H_sH_p = H_pH_s$ and so we conclude from the corollaries of Lemmas 12 and 15 that

$$(1) \qquad \sum_{1\leqq i\leqq r} (q_{kis}q_{ijp} - q_{kip}q_{ijs}) \equiv 0 \bmod \mathfrak{B}\mathfrak{k} \qquad (1 \leqq k, j \leqq r; 1 \leqq p, s \leqq l_0).$$

Moreover from Lemma 16, we can select a positive integer N and elements $g_{pja} \in \mathfrak{R}$, $\tau_{pja} \in \mathfrak{M}$ $(1 \leqq p \leqq l_0, 1 \leqq j \leqq r, 1 \leqq a \leqq N)$ such that

$$(2) \qquad \phi(m; H_p\nu_j) = \sum_{1 \leqq i \leqq r} \phi(m; \nu_i q_{ijp}) + \sum_{1 \leqq a \leqq N} g_{pja}(m)\phi(m; \tau_{pja}) \qquad (m \in M')$$

for any spherical function ϕ on G of class C^∞ $(1 \leqq j \leqq r, 1 \leqq p \leqq l_0)$.

6. Some rough estimates. Let $\mathfrak{F}$ be the space of all linear functions on $\mathfrak{h}_\mathfrak{p}$. For any $\lambda \in \mathfrak{F}$, put

$$\phi_\lambda(x) = \phi(\lambda : x) = \int_K \exp\{(-1)^{\frac{1}{2}}\lambda(H(xk)) - \rho(H(xk))\}dk \qquad (x \in G)$$

in the notation of Lemma 3 of [2(i)]. For $m \in M$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$ we write

$$\Phi_j(\lambda : m : H) = e^{\rho(H)}\phi(\lambda : m \exp H; \nu_j) \qquad (1 \leqq j \leqq r)$$

and

$$\Psi_{pj}(\lambda : m : H) = e^{\rho(H)} \sum_{1 \leqq a \leqq N} g_{pja}(m \exp H)\phi(\lambda : m \exp H; \tau_{pja}) \qquad (1 \leqq j \leqq r, 1 \leqq p \leqq l_0)$$

where g_{pja} and τ_{jpa} have the same meaning as in equation (2) of Section 5 and m, H are so chosen that $m \exp H \in M'$. Now let $\Phi(\lambda : m : H)$ and $\Psi_p(\lambda : m : H)$ denote the corresponding one-column matrices and define the $r \times r$ matrices $\Xi_p(\lambda)$ $(1 \leqq p \leqq l_0)$ by $\Xi_{pij}(\lambda) = \gamma(q_{jip} : (-1)^{\frac{1}{2}}\lambda)$ $(1 \leqq i, j \leqq r)$. Then it follows from equation (1) that $\Xi_p(\lambda)$ $(1 \leqq p \leqq l_0)$ commute with each other. For any $H' \in \mathfrak{l}$, put

$$\Psi_{H'}(\lambda : m : H) = \sum_p c_p \Psi_p(\lambda : m : H), \qquad \Xi(\lambda : H') = \sum_p c_p \Xi_p(\lambda) + \rho(H')I$$

where $H' = \sum_p c_p H_p$ $(c_p \in C)$ and I is the unit matrix. If $m \in M_+$ and $H \in \mathfrak{l}_0^+$, it is obvious that $m \exp tH \in M_+$ for all $t \geqq 0$. Therefore from Lemma 18 of [2(i)] and equation (2), we find that

$$d\Phi(\lambda : m : tH)/dt = \Xi(\lambda : H)\Phi(\lambda : m : tH) + \Psi_H(\lambda : m : tH) \qquad (t \geqq 0).$$

The following lemma is now obvious.

LEMMA 17.

$$d\Phi(\lambda : m; \eta : tH)/dt = \Xi(\lambda : H)\Phi(\lambda : m; \eta : tH) + \Psi_H(\lambda : m; \eta : tH)$$

for $\lambda \in \mathfrak{F}$, $m \in M_+$, $H \in \mathfrak{l}_0^+$, $\eta \in \mathfrak{M}$ *and* $t \geqq 0$.

Now put $\Phi^0(\lambda:m:H)=\exp(-\Xi(\lambda:H))\Phi(\lambda:m:H)$ and

$$\Psi_{H'}{}^0(\lambda:m:H)=\exp(-\Xi(\lambda:H))\Psi_{H'}(\lambda:m:H) \qquad (H'\in\mathfrak{l}).$$

COROLLARY. *$d\Phi^0(\lambda:m;\eta:tH)/dt=\Psi_H{}^0(\lambda:m;\eta:tH)$ under the conditions of Lemma 17.*

This is an immediate consequence of the above lemma.

For any $p\times q$ matrix $u=(u_{ij})$ with complex coefficients, put $\|u\| =\{\sum_{i,j}|u_{ij}|^2\}^{\frac{1}{2}}$. We now intend to obtain an estimate for $\|\Psi_H{}^0(\lambda:m;\eta:tH)\|$. It follows from Lemma 46 of [2(i)] and Lemma 7 that for any fixed η, we can choose an integer $k\geqq 0$ and a positive number a' such that[2]

$$\|\Psi_p(\lambda:m;\eta:H)\|$$
$$\leqq a'(1+\|\lambda\|)^k\,|\operatorname{Ad}(h^{-1}m^{-1})|_+{}^2\{1-|\operatorname{Ad}(h^{-1}m^{-1})|_+{}^2\}^{-(k+1)}e^{\rho(H)}\phi((-1)^{\frac{1}{2}}\lambda_I:mh)$$

for $m\in M_+$, $H\in\mathfrak{l}_0{}^+$, $\lambda\in\mathfrak{F}$ and $1\leqq p\leqq l_0$. (Here $h=\exp H$.) Now put $\beta(H)=\min_{\alpha\in Q}\alpha(H)$ and $A_{\mathfrak{l}}{}^+=\exp\mathfrak{l}_0{}^+$. Then

$$|\operatorname{Ad}(h^{-1}m^{-1})|_+\leqq|\operatorname{Ad}(m^{-1})|_+e^{-\beta(\log h)}\leqq e^{-\beta(\log h)}$$

for $m\in M_+$ and $h\in A_{\mathfrak{l}}{}^+$. Hence we get the following result immediately.

LEMMA 18. *For any $\eta\in\mathfrak{M}$, we can choose an integer $k\geqq 0$ and a positive number a such that*

$$\|\Psi_H(\lambda:mh;\eta:tH)\|$$
$$\leqq a(1+\|\lambda\|)^k\,\|H\|\exp\{t\rho(H)-t\beta(H)-\beta(\log h)\}\phi((-1)^{\frac{1}{2}}\lambda_I:mh\exp tH)$$

for $\lambda\in\mathfrak{F}$, $m\in M_+$, $h\in A_{\mathfrak{l}}{}^+$, $H\in\mathfrak{l}_0{}^+$ and $t\in R$ provided $t\beta(H)+\beta(\log h)\geqq 1$.

On the other hand

$$\|\Psi_H{}^0(\lambda:m;\eta:tH)\|\leqq\|\exp(-t\Xi(\lambda:H))\|\,\|\Psi_H(\lambda:m;\eta:tH)\|.$$

So now we have to estimate $\|\exp(-t\Xi(\lambda:H))\|$. Put $\lambda^*=(-1)^{\frac{1}{2}}\lambda$ for $\lambda\in\mathfrak{F}$.

LEMMA 19. *Select r elements $s_1,s_2,\cdots,s_r$ in W such that $W=\bigcup_{1\leqq i\leqq r}W's_i$. Then if T is an indeterminate and I the $r\times r$ unit matrix,*

$$\det(TI-\Xi(\lambda:H))=\prod_{1\leqq i\leqq r}(T-\lambda^*(s_iH))$$

for $\lambda\in\mathfrak{F}$ and $H\in\mathfrak{l}$.

Fix λ and H and select $q_{ij}\in I_{\mathfrak{g}}$ $(1\leqq i,j\leqq r)$ such that $H\nu_j\equiv\sum_i\nu_i\mu_0(q_{ij})$

mod $\mathfrak{M}\mathfrak{m}_{\mathfrak{l}}$. Since $\mathfrak{l}$ is contained in the center of $\mathfrak{m}$, it follows by applying the homomorphism $\gamma_{\mathfrak{m}}$ to this relation that $Hv_j' = \sum_i v_i'\gamma_{\mathfrak{m}}(\mu_0(q_{ij}))$ where $v_i' = \gamma_{\mathfrak{m}}(\nu_i)$. Moreover $e^{\rho-\sigma}H \circ e^{-\rho+\sigma} = H - \rho(H)$ since σ is zero on $\mathfrak{l}$. So if $v_i = e^{\rho-\sigma}v_i' \circ e^{-\rho+\sigma}$, it follows from Lemma 12 that $Hv_j = \rho(H)v_j + \sum_i v_i\gamma(q_{ij})$. Now if we recall the definition of the matrix $\Xi(\lambda:H)$ and denote its coefficients by ξ_{ij}, it becomes clear that

$$Hv_j \equiv \sum_i \xi_{ji} v_i \bmod J'J_\lambda.$$

in the notation of Lemma 13 of [2(i)]. But it follows from our definition of $\nu_1, \cdots, \nu_r$ and this lemma that $v_1, \cdots, v_r$ are linearly independent mod $J'J_\lambda$. Hence our assertion is an immediate consequence of the corollary of Lemma 15 of [2(i)].

COROLLARY. *There exists a positive number a and an integer $k \geqq 0$ such that*

$$\| \exp(t\Xi(\lambda:H)) \| \leqq a(1 + \|\lambda\|)^k (1 + |t|)^r (1 + \|H\|)^r \times \exp\{2r\,|t| \max_{1 \leqq i \leqq r} |\lambda_I(s_i H)|\}$$

for $H \in \mathfrak{l}_0$, $t \in R$ and $\lambda \in \mathfrak{F}$.

It follows from the definition of $\Xi(\lambda:H)$ that we can choose a positive number b and an integer $d \geqq 0$ such that

$$\| \Xi(\lambda:H) \| \leqq b(1 + \|\lambda\|)^d \|H\| \qquad (\lambda \in \mathfrak{F}, H \in \mathfrak{l}).$$

Moreover it follows from the above lemma and [2(i), Lemma 60] that

$$\| \exp(t\Xi(\lambda:H)) \| \leqq r^{\frac{1}{2}} \exp(2r\,|t| \max_{1 \leqq i \leqq r} |\lambda_I(s_i H)|) \sum_{0 \leqq k \leqq r} |t|^k \| \Xi(\lambda:H) \|^k.$$

Therefore the statement of the corollary is now obvious.

For a positive number ϵ, let $\mathfrak{F}_\epsilon$ denote the set of all $\lambda \in \mathfrak{F}$ such that $\|\lambda_I\| < \epsilon$.

LEMMA 20. *Let V be a compact set in $\mathfrak{l}_0^+$. Then there exists a positive number ϵ with the following property. Let η be an element in $\mathfrak{M}$. Then we can choose an integer $k \geqq 0$ and, for any compact set ω in M_+, positive numbers a_1, a_2 and t_0 such that*

$$\| \Psi_H{}^0(\lambda: mh; \eta: tH) \| \leqq a_1(1 + \|\lambda\|)^k t^k e^{-a_2 t}$$

for $\lambda \in \mathfrak{F}_\epsilon$, $m \in \omega$, $h \in A_{\mathfrak{l}}{}^+$, $H \in V$ and $t \geqq t_0$.

Our proof depends on Lemma 18. But first we need an estimate for $\phi((-1)^{\frac{1}{2}}\lambda_I : mh)$.

Lemma 21. *Let ϵ' be a positive number < 1. Then we can select an integer $d \geqq 0$ and positive numbers ϵ and a such that*

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh) \leqq a(1 + \| \log h \|)^d e^{-(1-\epsilon')\rho(\log h)}$$

for $m \in \omega$, $h \in A_{\mathfrak{I}}^+$ and $\lambda \in \mathfrak{F}_\epsilon$. Moreover d and ϵ may be so chosen that they are independent of ω.

From Theorem 3 and Lemma 49 of [2(i)], we can select d, ϵ and a positive number a' such that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : \exp H) \leqq a'(1 + \| H \|)^d e^{-(1-\epsilon')\rho(H)}$$

if $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand since ϕ_μ is a spherical function for any $\mu \in \mathfrak{F}$, it is obvious that $\phi((-1)^{\frac{1}{2}}\lambda_I : \exp H) = \phi((-1)^{\frac{1}{2}}\lambda_I : \exp sH)$ $(s \in W, H \in \mathfrak{h}_{\mathfrak{p}_0})$. Moreover $\rho(H) \geqq \rho(sH)$ for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$. Therefore since $\mathfrak{h}_{\mathfrak{p}_0} = \bigcup_{s \in W} s(\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+))$ (see [2(*f*), Lemma 37]), we conclude that the above inequality actually holds for all $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

On the other hand $M = M_K A_{\mathfrak{p}} M_K$ (see [2(f), Lemmas 31 and 33]) and since ω is compact, we can select a positive number c such that[10] $\| \log | m | \| \leqq c$ for $m \in \omega$. For a fixed $m \in \omega$, choose $h_1 \in A_{\mathfrak{p}}$ such that $m \in M_K h_1 M_K$. Then $\| \log h_1 \| = \| \log | m | \| \leqq c$ and

$$\begin{aligned} \phi((-1)^{\frac{1}{2}}\lambda_I : mh) &= \phi((-1)^{\frac{1}{2}}\lambda_I : h_1 h) \\ &\leqq a'(1 + \| \log(h_1 h) \|)^d \exp\{-(1-\epsilon')\rho(\log(h_1 h))\} \end{aligned}$$

if $h \in A_{\mathfrak{I}}^+$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand we can select a positive number a'' such that

$$(1 + \| H \|)^d e^{-(1-\epsilon')\rho(H)} \leqq a''$$

for all elements $H \in \mathfrak{h}_{\mathfrak{p}_0}$ with $\| H \| \leqq c$. Then if $a = a'a''$, it follows that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh) \leqq a(1 + \| \log h \|)^d e^{-(1-\epsilon')\rho(\log h)}$$

for $m \in \omega$, $h \in A_{\mathfrak{I}}^+$ and $\lambda \in \mathfrak{F}_\epsilon$.

Now we come to the proof of Lemma 20. Since V is compact, we can choose a positive number a_2 such that $\beta(H) \geqq 2a_2$ for $H \in V$. Put $t_0 = \max(1, a_2^{-1})$ and select ϵ and ϵ' as in Lemma 21. We can assume that ϵ and ϵ' are so small that $\epsilon'\rho(H) \leqq a_2/2$ and $2r | \lambda_I(sH) | \leqq a_2/2$ for $H \in V$,

---

[10] For any $x \in G$, $| x |$ denotes the unique element $p \in \exp \mathfrak{p}_0$ such that $xp^{-1} \in K$. Moreover $\log | x | = X$ where $| x | = \exp X$ $(X \in \mathfrak{p}_0)$.

$s \in W$ and $\lambda \in \mathfrak{F}_\epsilon$. Therefore it follows from Lemma 18 and the corollary of Lemma 19 that we can select an integer $k_1 \geqq 0$ and a positive number a' such that

$$\begin{aligned}&\| \Psi_H{}^0(\lambda : m;\eta : tH) \| \\ &\qquad \leqq a'(1+\|\lambda\|)^{k_1} t^r \exp\{t\rho(H) - 3ta_2/2\}\phi((-1)^{\frac{1}{2}}\lambda_I : m \exp tH)\end{aligned}$$

if $m \in M_+$, $H \in V$, $t \geqq t_0$ and $\lambda \in \mathfrak{F}_\epsilon$. On the other hand by Lemma 21,

$$\begin{aligned}&\phi((-1)^{\frac{1}{2}}\lambda_I : mh \exp tH) \\ &\qquad \leqq a(1+t\|H\|)^d e^{-(1-\epsilon')t\rho(H)}(1+\|\log h\|)^d\, e^{-(1-\epsilon')\rho(\log h)}\end{aligned}$$

for $m \in \omega$, $h \in A_I{}^+$ and $t \geqq t_0$. Moreover it is obvious that there exists a positive number c such that $\rho(H') \geqq c\|H'\|$ for $H' \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. Therefore since $(1+t)^d e^{-(1-\epsilon')ct} \to 0$ as $t \to +\infty$, we can select a number $a'' > 0$ such that

$$\phi((-1)^{\frac{1}{2}}\lambda_I : mh \exp tH) \leqq a'' t^d e^{-(1-\epsilon')t\rho(H)}$$

for $m \in \omega$, $h \in A_I{}^+$, $t \geqq t_0$ and $\lambda \in \mathfrak{F}_\epsilon$. This shows that

$$\| \Psi_H{}^0(\lambda : mh;\eta : tH)\| \leqq a'a''(1+\|\lambda\|)^{k_1} t^{r+d} \exp\{\epsilon' t\rho(H) - 3ta_2/2\}$$

under the same conditions. Therefore if we put $a_1 = a'a''$, $k = \max(k_1, r+d)$ and recall that $\epsilon'\rho(H) \leqq a_2/2$ for $H \in V$, the statement of Lemma 20 follows immediately.

7. The function Θ_H. Now fix an element H in $\mathfrak{l}_0{}^+$. Then if ϵ is sufficiently small, it follows from Lemma 20 and the corollary to Lemma 17 that for any $\eta \in \mathfrak{M}$, the integral

$$\int_0^\infty \| d\Phi^0(\lambda : m;\eta : tH)/dt \| \, dt$$

converges uniformly as m and λ vary within compact subsets of M_+ and $\mathfrak{F}_\epsilon$ respectively. This shows that $\lim\limits_{t\to+\infty} \Phi^0(\lambda : m : tH)$ exists and for a fixed m, it represents a holomorphic (matrix-) function of λ on $\mathfrak{F}_\epsilon$. We shall denote this limit by $\Theta_H(\lambda : m)$. Moreover in view of the uniform convergence of the above integral, the following facts are obvious. For a fixed λ in $\mathfrak{F}_\epsilon$, $\Theta_H(\lambda : m)$ is a C^∞ function of m on M_+ and $\Theta_H(\lambda : m;\eta) = \lim\limits_{t\to+\infty}\Phi^0(\lambda : m;\eta : tH)$ for $\eta \in \mathfrak{M}$. Now suppose ω is a compact subset of M. Then we can obviously select a positive number t_0 such that $m \exp t_0H \in M_+$ for $m \in \omega$. Also it follows from the definition of Φ^0 that

$$\Phi^0(\lambda : m : tH + t_0H) = e^{t_0\rho(H)} \exp\{-t_0\Xi(\lambda : H)\}\Phi^0(\lambda : m \exp t_0H : tH).$$

Therefore if $\lambda \in \mathfrak{F}_\epsilon$ and $m \in \omega$,

$$\operatorname*{Lim}_{t \to +\infty} \Phi^0(\lambda : m : tH) = e^{t_0\rho(H)} \exp\{-t_0\Xi(\lambda : H)\}\Theta_H(\lambda : m \exp t_0 H).$$

Hence we can extend Θ_H on $\mathfrak{F}_\epsilon \times M$ by setting

$$\Theta_H(\lambda : m) = \operatorname*{Lim}_{t \to +\infty} \Phi^0(\lambda : m : tH) \qquad (\lambda \in \mathfrak{F}_\epsilon, m \in M).$$

The following result is now obvious.

LEMMA 22. *$\Theta_H(\lambda : m \exp tH) = e^{-t\rho(H)} \exp(t\Xi(\lambda : H))\Theta_H(\lambda : m)$ for $t \in R$, $m \in M$ and $\lambda \in \mathfrak{F}_\epsilon$.*

This lemma shows that for a fixed λ in $\mathfrak{F}_\epsilon$, Θ_H is a C^∞ function on M and for a fixed m in M, it is a holomorphic function on $\mathfrak{F}_\epsilon$.

LEMMA 23. *For any $\eta \in \mathfrak{M}$ we can select an integer k such that $(1 + \|\lambda\|)^{-k} \|\Theta_H(\lambda : m ; \eta)\|$ remains bounded for any fixed $m \in M$ as λ varies in $\mathfrak{F}_\epsilon$.*

Select $t_0 > 0$ such that $m_0 = m \exp t_0 H \in M_+$. Then

$$\Theta_H(\lambda : m ; \eta) = e^{t_0\rho(H)} \exp\{-t_0\Xi(\lambda : H)\}\Theta_H(\lambda : m_0 ; \eta).$$

Hence in view of the corollary to Lemma 19, it is sufficient to consider the case when $m \in M_+$. But then

$$\Theta_H(\lambda : m ; \eta) = \Phi^0(\lambda : m ; \eta : TH) + \int_T^\infty \Psi_H{}^0(\lambda : m ; \eta : tH)\, dt$$

for $T \geqq 0$. Therefore

$$\|\Theta_H(\lambda : m ; \eta)\| \leqq \|\exp(-T\Xi(\lambda : H))\| \, \|\Phi(\lambda : m ; \eta : TH)\| + \int_T^\infty \|\Psi_H{}^0(\lambda : m ; \eta : tH)\|\, dt.$$

On the other hand it follows from Lemma 46 of [2(i)] that

$$\|\Phi(\lambda : m ; \eta : TH)\| \leqq a_1(1 + \|\lambda\|)^{k_1}\phi((-1)^{\frac{1}{2}}\lambda_I : m \exp TH)e^{T\rho(H)} \qquad (\lambda \in \mathfrak{F}_\epsilon, T \geqq 0)$$

where a_1 is a positive number and k_1 a nonnegative integer and the latter depends only on η. Hence if we apply Lemmas 20 and 21 and take into account the corollary of Lemma 19, our assertion becomes obvious.

Choose $\epsilon' > 0$ such that $\epsilon'\rho(H) < \beta(H)/3$ and $\epsilon' < 1$. We assume that ϵ is so small that the pair (ϵ, ϵ') fulfills the condition of Lemma 21 and $6r\epsilon \|H\| < \beta(H)$.

LEMMA 24. *Let q be an element in $I_{\mathfrak{g}}$. Then*

$$\Theta_H(\lambda : m ; \mu_0(q)) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda : m)$$

for $\lambda \in \mathfrak{F}_\epsilon$ *and* $m \in M$.

In view of Lemma 22, we may assume that $m \in M_+$. Now

$$\phi(\lambda : m ; \nu_i\mu_0(q)) = \phi(\lambda : m ; \nu_i q) - \phi(\lambda : m ; \nu_i \circ \mu(q)) \qquad (1 \leqq i \leqq r)$$

in the notation of Section 5. But $\phi(\lambda : m ; \nu_i q) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\phi(\lambda : m ; \nu_i)$ and $\nu_i\mu_0(q) - \mu_0(q)\nu_i \in \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$ by Theorem 1 of [2(i)] since $\mu_0(q) \in I_{\mathfrak{m}}$. Therefore

$$\phi(\lambda : m ; \mu_0(q)\nu_i) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\phi(\lambda : m ; \nu_i) - \phi(\lambda : m ; \nu_i \circ \mu(q)).$$

Now fix m and λ. Then it follows from Lemmas 7 and 21 and [2(i), Lemma 46] that

$$|\phi(\lambda : m \exp tH ; \nu_i \circ \mu(q))| \leqq a(1+t)^d \exp\{-t\beta(H) - (1-\epsilon')t\rho(H)\} \qquad (t \geqq 0)$$

where a is a positive constant. Hence we can select a constant a_1 such that

$$\|\Phi(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi(\lambda : m : tH)\| \leqq a_1(1+t)^d e^{-2t\beta(H)/3} \qquad (t \geqq 0).$$

Therefore

$$\|\Phi^0(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi^0(\lambda : m : tH)\| \leqq a_1(1+t)^d e^{-2t\beta(H)/3} \|\exp(-t\Xi(\lambda : H))\|.$$

In view of the inequality $6r\epsilon\|H\| \leqq \beta(H)$, it follows from the corollary of Lemma 19 that

$$\lim_{t\to+\infty} \|\Phi^0(\lambda : m ; \mu_0(q) : tH) - \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Phi^0(\lambda : m : tH)\| = 0.$$

This proves that $\Theta_H(\lambda : m ; \mu_0(q)) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda : m)$.

COROLLARY. *For a fixed* λ *in* $\mathfrak{F}_\epsilon$, $\Theta_H(\lambda : m)$ *is an analytic function of* m *on* M.

Let $Y_1, \cdots, Y_s$ be an orthonormal base for $\mathfrak{m}_{\mathfrak{k}_0}$ over R. Then it is easy to verify that $Y_1^2 + \cdots + Y_s^2 \in I_{\mathfrak{m}}$ and if ω is the Casimir operator of $\mathfrak{g}$, it follows from Lemma 14 that $\eta = \mu_0(\omega) + Y_1^2 + \cdots + Y_s^2$ is an elliptic differential operator (see Garding [1] for the definition of ellipticity) on M. On the other hand it is obvious from the definition of Θ_H that $\Theta_H(\lambda : k_1 m k_2)$

$= \Theta_H(\lambda : m)$ for $k_1, k_2 \in M_K$. Therefore $\Theta_H(\lambda : m ; \eta) = \Theta_H(\lambda : m ; \mu_{\mathfrak{g}}(\omega))$ $= \gamma(\omega : (-1)^{\frac{1}{2}}\lambda)\Theta_H(\lambda : m)$. This shows that for a fixed λ, every coefficient of the matrix Θ_H is an eigenfunction of η. Therefore since η is an analytic differential operator on M of the elliptic type, we can conclude (see John [3]) that all these coefficients are also analytic in m.

We shall now try to determine Θ_H explicitly.

LEMMA 25. *Let θ' be an analytic function on M such that $\theta'(k_1 m k_2)$ $= \theta'(m)$ for $k_1, k_2 \in M_K$ and $m \in M$ and suppose θ' is an eigenfunction of $\mu_0(q)$ for every $q \in I_{\mathfrak{g}}$. Then the equations $\theta'(1 ; \nu_i) = 0$ $(1 \leqq i \leqq r)$ imply that θ' is identically zero.*

Let η be any element in $\mathfrak{M}$. Put $\eta_0 = \int_{M_K} \eta^{k'}\, dk'$ where dk' denotes the normalized Haar measure on M_K. It is clear that $\theta'(1 ; \eta) = \theta'(1 ; \eta_0)$. But $\eta_0 \in I_{\mathfrak{m}}$ and $I_{\mathfrak{m}} \subset \sum_i \nu_i \mu_0(I_{\mathfrak{g}}) + \mathfrak{M}\mathfrak{m}_{\mathfrak{k}}$ from Lemma 15. Hence it follows from our assumptions that $\theta'(1 ; \eta_0) = 0$. This shows that $\theta'(1 ; \eta) = 0$ for every $\eta \in \mathfrak{M}$. But since θ' is analytic, this means that $\theta' = 0$.

For any $\lambda \in \mathfrak{F}$, put

$$\theta_\lambda(m) = \theta(\lambda : m) = \int_{M_K} \exp\{(-1)^{\frac{1}{2}}\lambda(H(mk')) - \rho(H(mk'))\}\, dk' \qquad (m \in M)$$

where dk' has the same meaning as above. Define $\gamma_{\mathfrak{m}}'(\eta) = e^{\rho - \sigma}\gamma_{\mathfrak{m}}(\eta) \circ e^{-\rho + \sigma}$ for $\eta \in I_{\mathfrak{m}}$ as in Section 5. Then by applying Lemma 18 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$), it follows without difficulty that

$$\theta(\lambda : m ; \eta) = \gamma_{\mathfrak{m}}'(\eta : (-1)^{\frac{1}{2}}\lambda)\theta(\lambda : m) \qquad (\eta \in I_{\mathfrak{g}}),$$

where $\gamma_{\mathfrak{m}}'(\eta : (-1)^{\frac{1}{2}}\lambda)$ denotes the value of the polynomial function $\gamma_{\mathfrak{m}}'(\eta)$ $\in S(\mathfrak{h}_{\mathfrak{p}})$ at $(-1)^{\frac{1}{2}}\lambda$. Therefore

$$\theta(\lambda : m ; \mu_0(q)) = \gamma(q : (-1)^{\frac{1}{2}}\lambda)\theta(\lambda : m) \qquad (q \in I_{\mathfrak{g}})$$

from Lemma 12.

Put $v_i = \gamma_{\mathfrak{m}}'(\nu_i)$ $1 \leqq i \leqq r$ and define π, π', $D = \pi/\pi'$ and τ^i $(1 \leqq i \leqq r)$ as in Lemma 15 of [2(i)]. Also put $\lambda^* = (-1)^{\frac{1}{2}}\lambda$ $(\lambda \in \mathfrak{F})$.

LEMMA 26. *Select r elements $s_1 = 1, s_2, \cdots, s_r$ in W such that $W = \bigcup_{1 \leqq i \leqq r} W' s_i$. Then*

$$\pi(\lambda^*)\Theta_H(\lambda : m) = \sum_{1 \leqq i, j \leqq r} \epsilon(s_i)\pi'(s_i\lambda^*)\tau^j(s_i\lambda^*)\Theta_H(\lambda : 1 ; \nu_j)\theta(s_i\lambda : m)$$

for $\lambda \in \mathfrak{F}_\epsilon$ and $m \in M$.

For a fixed m, both sides are holomorphic functions of λ. Hence it is enough to prove the above relation under the assumption that $\pi(\lambda) \neq 0$. Put $\lambda_i = s_i\lambda$. Then the rational functions $v^k = \tau^k/D$ on $\mathfrak{h}_{\mathfrak{p}}$ $(1 \leqq k \leqq r)$ are all defined at λ_i^* and we have to show that

$$f(\lambda:m) = \Theta_H(\lambda:m) - \sum_{1\leqq i,j\leqq r} v^j(\lambda_i^*)\Theta_H(\lambda:1;\nu_j)\theta(\lambda_i:m)$$

is zero. On the other hand $\theta(\lambda_i:m;\nu_k) = v_k(\lambda_i^*)\theta(\lambda_i:m)$ and therefore

$$f(\lambda:1;\nu_k) = \Theta_H(\lambda:1;\nu_k) - \sum_{1\leqq i,j\leqq r} v^j(\lambda_i^*)\Theta_H(\lambda:1;\nu_j)v_k(\lambda_i^*).$$

But since $\mathrm{sp}_{J'/J}(v^j v_k) = \delta_k{}^j$ (see [2(i), § 3]), it follows that

$$\sum_i v^j(\lambda_i^*)v_k(\lambda_i^*) = \delta_k{}^j \qquad (1 \leqq j, k \leqq r)$$

and therefore $f(\lambda:1;\nu_k) = 0$ $(1 \leqq k \leqq r)$. Hence our assertion is a consequence of Lemma 25.

8. The function Θ. We shall now show that if $\lambda \in \mathfrak{F}_K$, $\Theta_H(\lambda:m)$ is actually independent of H. Let H' be another element in $\mathfrak{l}_0^+$ and for a fixed $m \in M$, choose a positive number T_0' such that $m \exp T_0'H' \in M_+$. Then

$$\begin{aligned}\Phi^0(\lambda:m:TH+T'H') \\ &= \Phi^0(\lambda:m:T'H') + \int_0^T \{d\Phi^0(\lambda:m:tH+T'H')/dt\}dt\end{aligned}$$

for $T, T' \geqq 0$. On the other hand

$$\Phi^0(\lambda:m:tH+T'H') = e^{T'\rho(H')}\exp(-T'\Xi(\lambda:H'))\Phi^0(\lambda:m\exp T'H':tH)$$

from the definition of Φ^0. Therefore

$$\begin{aligned}\| d\Phi^0(\lambda:m:tH+T'H')/dt \| \\ &\leqq e^{T'\rho(H')}\|\exp(-T'\Xi(\lambda:H'))\| \, \|\Psi_H{}^0(\lambda:m\exp T'H':tH)\|\end{aligned}$$

for $t \geqq 0$ and $T' \geqq T_0'$. Now fix λ and m and assume that T_0' is sufficiently large. Then from Lemma 18 we can choose a constant a such that

$$\begin{aligned}\| d\Phi^0(\lambda:m:tH+T'H')/dt \| \\ &\leqq a e^{T'\rho(H')}\|\exp(-T'\Xi(\lambda:H'))\| \, \|\exp(-t\Xi(\lambda:H))\| \\ &\qquad\times\exp\{t\rho(H) - t\beta(H) - T'\beta(H')\}\phi(0:\exp(T'H'+tH))\end{aligned}$$

for $T' \geqq T_0'$ and $t \geqq 0$. Hence in view of Theorem 3 of [2(i)] and the corollary of Lemma 19, we can find a positive number c and an integer $k \geqq 0$ such that

$$\| d\Phi^0(\lambda:m:tH+T'H')/dt \| \leqq c(1+t)^k T'^k \exp\{-t\beta(H) - T'\beta(H')\} \qquad (T' \geqq T_0', t \geqq 0).$$

But this implies that

$$\lim_{T'\to+\infty}\int_0^\infty \| d\Phi^0(\lambda:m:tH+T'H')/dt \| \, dt = 0$$

and therefore $\Phi^0(\lambda:m:TH+T'H')$ converges to $\lim_{t'\to+\infty}\Phi^0(\lambda:m:t'H') = \Theta_{H'}(\lambda:m)$ as $T'\to+\infty$, uniformly with respect to T. Hence

$$\Theta_{H'}(\lambda:m) = \lim_{T,T'\to+\infty}\Phi^0(\lambda:m:TH+T'H').$$

But since the right side is symmetric with respect to H and H', we conclude that $\Theta_{H'}(\lambda:m) = \Theta_H(\lambda:m)$.

Now put $\Theta(\lambda:m) = \Theta_H(\lambda:m)$ $(\lambda\in\mathfrak{F}_R, m\in M)$ for any $H\in\mathfrak{l}_0^+$. We propose to obtain an estimate for the difference $\Phi^0-\Theta$.

LEMMA 27. *For any $\eta\in\mathfrak{M}$, we can choose an integer $k\geqq 0$ and a positive constant a such that*

$$\begin{aligned}&\| \Phi^0(\lambda:h;\eta:H)-\Theta(\lambda:h;\eta)\| \\ &\qquad \leqq a(1+\|\lambda\|)^k(1+\|H\|)^k e^{-\beta(H)}(1+\|\log h\|)^d e^{-\rho(\log h)}\end{aligned}$$

for $\lambda\in\mathfrak{F}_R$, $h\in A_\mathfrak{p}^+$ and $H\in\mathfrak{l}_0^+$, provided $\beta(H)\geqq 1$. (Here d has the same meaning as in [2(i), Theorem 3].)

We know that

$$\Theta(\lambda:h;\eta) = \Phi^0(\lambda:h;\eta:H) + \int_1^\infty \{d\Phi^0(\lambda:h;\eta:tH)/dt\}dt.$$

Moreover

$$\begin{aligned}\| d\Phi^0(\lambda:h;\eta:tH)/dt\| &= \|\Psi_H{}^0(\lambda:h;\eta:tH)\| \\ &\leqq \|\exp(-t\Xi(\lambda:H))\| \, \|\Psi_H(\lambda:h;\eta:tH)\|.\end{aligned}$$

Therefore it follows from Lemma 18 and the corollary to Lemma 19, that we can select integers $k_1, k_2\geqq 0$ and a positive number c_1 such that

$$\begin{aligned}&\| d\Phi^0(\lambda:h;\eta:tH)/dt\| \\ &\qquad \leqq c_1(1+\|\lambda\|)^{k_1}t^{k_2}(1+\|H\|)^{k_2}\exp\{t\rho(H)-t\beta(H)\}\phi(0:h\exp tH)\end{aligned}$$

for $\lambda\in\mathfrak{F}_R$, $h\in A_\mathfrak{p}^+$, $H\in\mathfrak{l}_0^+$ and $t\geqq 1$ provided $\beta(H)\geqq 1$. On the other hand by Theorem 3 of [2(i)],

$$\phi(0:h\exp tH) \leqq c_2(1+\|\log h\|)^d(1+\|H\|)^d\exp\{-t\rho(H)-\rho(\log h)\}$$

where c_2 is a constant. Therefore

$$\begin{aligned}\| d\Phi^0(\lambda:h;\eta:tH)/dt\| &\leqq c_1c_2(1+\|\lambda\|)^{k_1}t^{k_2}(1+\|H\|)^{k_2+d} \\ &\qquad \times\exp\{-t\beta(H)-\rho(\log h)\}(1+\|\log h\|)^d.\end{aligned}$$

But

$$\int_1^\infty t^{k_2}e^{-t\beta(H)}dt = e^{-\beta(H)}\int_0^\infty (1+t)^{k_2}e^{-t\beta(H)}dt$$
$$\leqq e^{-\beta(H)}\int_0^\infty (1+t)^{k_2}e^{-t}\,dt,$$

since $\beta(H) \geqq 1$. Therefore our assertion is now obvious.

COROLLARY. *For a given $\eta \in \mathfrak{M}$, we can chose an integer $k_1 \geqq 0$ and a positive number a_1 such that*

$$\| \Phi(\lambda : h ; \eta : H) - \exp \Xi(\lambda : H)\Theta(\lambda : h ; \eta) \|$$
$$\leqq a_1(1 + \| \lambda \|)^{k_1}(1 + \| H \|)^{k_1} e^{-\beta(H)}(1 + \| \log h \|)^{d} e^{-\rho(\log h)}$$

for $\lambda \in \mathfrak{F}_R$, $h \in A_{\mathfrak{p}}^-$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$.

This is an immediate consequence of the above lemma and the corollary to Lemma 19.

9. The functions $\boldsymbol{b}$ and $\boldsymbol{b}_0$. Define $\boldsymbol{b}$ as in Lemma 52 of [2(i)]. We intend to show that $|\boldsymbol{b}(s\lambda)| = |\boldsymbol{b}(\lambda)|$ for $s \in W$ and $\lambda \in \mathfrak{F}_R$. Let us say that $h \to \infty$ ($h \in A_{\mathfrak{p}}^+$) if $\alpha(\log h) \to +\infty$ for every $\alpha \in P_+$. Moreover if f and g are two functions on $A_{\mathfrak{p}}^+$, we write $f(h) \sim g(h)$ if $\lim_{h\to\infty} |f(h) - g(h)| = 0$.

We now use the notation of Sections 7 and 8 and assume that ϵ is sufficiently small. Let $\mathfrak{F}_\epsilon'$ denote the set of those points $\lambda \in \mathfrak{F}_\epsilon$ where $\pi(\lambda) \neq 0$. Then it follows from Lemma 37 of [2(i)] (applied to $\mathfrak{m}$ instead of $\mathfrak{g}$) that there exists a holomorphic function $\boldsymbol{c}'$ on $\mathfrak{F}_\epsilon'$ such that[11]

$$e^{\rho(\log h)}\theta(\lambda : h) \sim \sum_{s \in W} \boldsymbol{c}'(s\lambda)\exp\{s\lambda^*(\log h)\} \qquad (h \in A_{\mathfrak{p}}^+)$$

for $\lambda \in \mathfrak{F}_\epsilon'$. Now let $\mathfrak{F}_R' = \mathfrak{F}_\epsilon' \cap \mathfrak{F}_R$ and fix $\lambda \in \mathfrak{F}_R'$ and $H \in \mathfrak{l}_0^+$. Put $\lambda_i = s_i\lambda$ and $f_i = f_{\lambda_i^*}$ $(1 \leqq i \leqq r)$ in the notation of [2(i), Lemma 15]. Define the $r \times r$ matrix $F(i)$ with complex coefficients by

$$f_i v_j \equiv \sum_k F_{jk}(i)v_k \bmod SJ_{\lambda^*}.$$

Then if I is the unit matrix of degree r, it follows from Lemma 15 of [2(i)] that $\sum_i \epsilon(s_i)\pi'(\lambda_i^*)F(i) = \pi(\lambda^*)I$ and $F(i)\Xi(\lambda : h) = \lambda_i^*(H)F(i)$ $1 \leqq i \leqq r$. Hence

$$\pi(\lambda^*)\Phi^0(\lambda : h : tH) = \pi(\lambda^*)\exp(-t\Xi(\lambda : H))\Phi(\lambda : h : tH)$$
$$= \sum_i \epsilon(s_i)\pi'(\lambda_i^*)e^{-t\lambda_i^*(H)}F(i)\Phi(\lambda : h : tH) \qquad (t \in R, h \in A_{\mathfrak{p}}).$$

---

[11] If $s \in W$ and $\mu \in \mathfrak{F}$, $s\mu(H')$ denotes the value of the linear function $s\mu$ at $H' \in \mathfrak{h}_{\mathfrak{p}}$.

Therefore

$$\pi(\lambda^*)\Theta(\lambda:h)=\lim_{t\to+\infty}\sum_i \epsilon(s_i)\pi'(\lambda_i^*)e^{-t\lambda_i^*(H)}F(i)\Phi(\lambda:h:tH).$$

Now put $\phi'(\lambda:h)=e^{\rho(\log h)}\phi(\lambda:h)$. Since $v_i=\gamma_{\mathfrak{m}}'(\nu_i)$ $(1\leqq i\leqq r)$, it follows without difficulty by applying Lemma 26 of [2(i)] to $\mathfrak{m}$ (in place of $\mathfrak{g}$) that

$$\lim_{t\to+\infty}|\Phi_j(\lambda:h:tH)-\phi'(\lambda:h\exp tH;v_j)|=0$$

for $h\in A_{\mathfrak{p}}^+$. Therefore

$$\begin{aligned}\pi(\lambda^*)e^{\rho(\log h)}\Theta_k(\lambda:h)&\\ =\lim_{t\to+\infty}\sum_{1\leqq i,j\leqq r}&\epsilon(s_i)\pi'(\lambda_i^*)e^{-t\lambda_i^*(H)}F_{kj}(i)\phi'(\lambda:h\ \exp tH;v_j).\end{aligned}$$

On the other hand it follows from Lemma 37 of [2(i)] that

$$\lim_{\substack{t\to+\infty\\ h\to\infty}}|\phi'(\lambda:h\exp tH;v_j)-\sum_{s\in W}\boldsymbol{c}(s\lambda)v_j(s\lambda^*)\exp\{s\lambda^*(\log h+tH)\}|=0.$$

But we know from [2(i), Lemma 15] that $f_iv_k\equiv v_k(\lambda_i^*)f_i \bmod SJ_{\lambda^*}$ and therefore

$$\sum_j F_{kj}(i)v_j(\lambda_m^*)=v_k(\lambda_i^*)f_i(\lambda_m^*)=v_k(\lambda_i^*)\delta_{im}D(\lambda_i^*)\qquad(1\leqq i,m\leqq r).$$

Moreover H is invariant under W', since it lies in the center of $\mathfrak{m}$. Hence

$$\begin{aligned}\sum_j F_{kj}(i)&\sum_{s\in W}\boldsymbol{c}(s\lambda)v_j(s\lambda^*)e^{s\lambda^*(\log h+tH)}\\ &=\sum_{j,m}F_{kj}(i)v_j(\lambda_m^*)\sum_{s'\in W'}\boldsymbol{c}(s'\lambda_m)e^{s'\lambda_m^*(\log h+tH)}\\ &=e^{t\lambda_i^*(H)}v_k(\lambda_i^*)D(\lambda_i^*)\sum_{s'\in W'}\boldsymbol{c}(s'\lambda_i)e^{s'\lambda_i^*(\log h)}.\end{aligned}$$

This proves that

$$\pi(\lambda^*)e^{\rho(\log h)}\Theta_k(\lambda:h)\sim\pi(\lambda^*)\sum_{1\leqq i\leqq r}v_k(\lambda_i^*)\sum_{s'\in W'}\boldsymbol{c}(s'\lambda_i)e^{s'\lambda_i^*(\log h)}\qquad(1\leqq k\leqq r).$$

Now put (in the notation of Lemma 26)[12]

$${}'\Gamma_{ki}(\lambda)=(-1)^{-d/2}\epsilon(s_i)\sum_{1\leqq j\leqq r}\tau^j(\lambda_i^*)\Theta_k(\lambda:1;\nu_j),$$

where d is the degree of $D=\pi/\pi'$. Then it follows from Lemma 26 that

$$\pi(\lambda)e^{\rho(\log h)}\Theta_k(\lambda:h)\sim\sum_{1\leqq i\leqq r}{}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\sum_{s'\in W'}\boldsymbol{c}'(s'\lambda_i)e^{s'\lambda_i^*(\log h)}.$$

This shows that

$$\lim_{h\to\infty}|\sum_i\sum_{s'\in W'}\{v_k(\lambda_i^*)\pi(\lambda)\boldsymbol{c}(s'\lambda_i)-{}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(s'\lambda_i)\}e^{s'\lambda_i^*(\log h)}|=0.$$

---

[12] For any integer k, $(-1)^{k/2}=((-1)^{\frac{1}{2}})^k$.

But since $\pi(\lambda) \neq 0$, the w elements $s'\lambda_i$ $(s' \in W', 1 \leqq i \leqq r)$ are all distinct. Hence we conclude from Lemma 57 of [2(i)] that

$$v_k(\lambda_i^*)\pi(\lambda)\boldsymbol{c}(s'\lambda_i) = {}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(s'\lambda_i) \qquad (s' \in W', 1 \leqq i, k \leqq r).$$

Putting $i = k = 1$ and ${}'\Gamma_{11} = \Gamma$, this becomes $\pi(\lambda)\boldsymbol{c}(s'\lambda) = \Gamma(\lambda)\pi'(\lambda)\boldsymbol{c}'(s'\lambda)$ $(\lambda \in \mathfrak{F}_R')$. Now if ϵ is sufficiently small, it follows from the results of Section 7, that ${}'\Gamma_{ij}$ can be extended to holomorphic functions on $\mathfrak{F}_\epsilon$. Moreover there exist (see [2(i), Lemma 52]) holomorphic functions $\boldsymbol{b}$ and $\boldsymbol{b}'$ on $\mathfrak{F}_\epsilon$ such that $\boldsymbol{b}(\lambda) = \pi(\lambda)\boldsymbol{c}(\lambda)$ and $\boldsymbol{b}'(\lambda) = \pi'(\lambda)\boldsymbol{c}'(\lambda)$ for $\lambda \in \mathfrak{F}_\epsilon'$. The above result shows that $\boldsymbol{b}(s'\lambda) = \Gamma(\lambda)\boldsymbol{b}'(s'\lambda)$ for $s' \in W'$ and $\lambda \in \mathfrak{F}_R'$. Hence by analytic continuation we obtain the following lemma.

LEMMA 28. $\boldsymbol{b}(s'\lambda) = \Gamma(\lambda)\boldsymbol{b}'(s'\lambda)$ *for* $s' \in W'$ *and* $\lambda \in \mathfrak{F}_\epsilon$.

COROLLARY 1. $|\boldsymbol{b}(s\lambda)| = |\boldsymbol{b}(\lambda)|$ *for* $s \in W$ *and* $\lambda \in \mathfrak{F}_R$.

It is obvious that $\phi(-\lambda : h) = \operatorname{conj} \phi(\lambda : h)$ for $\lambda \in \mathfrak{F}_R$ and $h \in A_\mathfrak{p}$. Hence it follows from Lemmas 37 and 57 of [2(i)] that $\boldsymbol{c}(-\lambda) = \operatorname{conj} \boldsymbol{c}(\lambda)$ for $\lambda \in \mathfrak{F}_R'$. Therefore if d is the degree of π, $\operatorname{conj} \boldsymbol{b}(\lambda) = (-1)^d \boldsymbol{b}(-\lambda)$ $(\lambda \in \mathfrak{F}_R)$. Let $l = \dim \mathfrak{h}_\mathfrak{p}$. If $l = 1$, W consists of only two elements. Hence if $s \neq 1$, $s\lambda = -\lambda$ and therefore our assertion is obvious. So now assume that $l \geqq 2$ and use induction. Define Σ as in [2(i), § 3]. Since the reflexions s_α $(\alpha \in \Sigma)$ generate W, it would be enough to prove that $|\boldsymbol{b}(s_\alpha\lambda)| = |\boldsymbol{b}(\lambda)|$ for $\alpha \in \Sigma$ and $\lambda \in \mathfrak{F}_R$. Now fix $\alpha \in \Sigma$ and select the element H_0 of Section 2 in such a way that $\alpha(H_0) = 0$. Then $s_\alpha \in W'$ and it follows by the induction hypothesis (applied to $\mathfrak{m}' = [\mathfrak{m}, \mathfrak{m}]$) that $|\boldsymbol{b}'(s'\lambda)| = |\boldsymbol{b}'(\lambda)|$ for $s' \in W'$ and $\lambda \in \mathfrak{F}_R$. But then by Lemma 27, $|\boldsymbol{b}(s_\alpha\lambda)| = |\Gamma(\lambda)\boldsymbol{b}'(s_\alpha\lambda)| = |\Gamma(\lambda)\boldsymbol{b}'(\lambda)| = |\boldsymbol{b}(\lambda)|$. This proves our assertion.

COROLLARY 2. $\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda) = \boldsymbol{b}(s\lambda)\boldsymbol{b}(-s\lambda)$ *for* $s \in W$ *and* $\lambda \in \mathfrak{F}_\epsilon$.

First suppose $\lambda \in \mathfrak{F}_R$. Then we have seen above that

$$\boldsymbol{b}(-\lambda) = (-1)^d \operatorname{conj} \boldsymbol{b}(\lambda)$$

and therefore

$$\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda) = (-1)^d |\boldsymbol{b}(\lambda)|^2 = (-1)^d |\boldsymbol{b}(s\lambda)|^2 = \boldsymbol{b}(s\lambda)\boldsymbol{b}(-s\lambda)$$

by Corollary 1. Hence the same identity holds for all $\lambda \in \mathfrak{F}_\epsilon$ by analytic continuation.

COROLLARY 3. *Suppose* ϵ *is sufficiently small. Then if* $\boldsymbol{b}(\lambda) = 0$ *for some* $\lambda \in \mathfrak{F}_\epsilon$, *it follows that* $\boldsymbol{b}(s\lambda) = 0$ *for every* $s \in W$.

If $l = 1$, our statement is true since $\boldsymbol{b}(\lambda)$ is never zero for $\lambda \in \mathfrak{F}_\epsilon$ (see Lemma 53 of [2(i)]). So let us assume that $l \geqq 2$ and use induction. Fix an element $\alpha \in \Sigma$. Obviously it would be enough to prove that $\boldsymbol{b}(s_\alpha\lambda) = 0$. Again choose H_0 in such a way that $s_\alpha \in W'$. If $\boldsymbol{b}'(\lambda) = 0$, it follows by induction hypothesis that $\boldsymbol{b}'(s_\alpha\lambda) = 0$. On the other hand if $\boldsymbol{b}'(\lambda) \neq 0$, $\Gamma(\lambda) = \boldsymbol{b}(\lambda)/\boldsymbol{b}'(\lambda) = 0$. Therefore in either case $\boldsymbol{b}(s_\alpha\lambda) = \Gamma(\lambda)\boldsymbol{b}'(s_\alpha\lambda) = 0$.

Now we regard $\mathfrak{F}_\epsilon$ as a complex-analytic manifold and consider the divisor $\boldsymbol{d}$ of the function $\boldsymbol{b}$ on $\mathfrak{F}_\epsilon$. Select $\alpha_1, \cdots, \alpha_q \in \Sigma$ such that $\pi = \alpha_1\alpha_2 \cdots \alpha_q$ and let $\boldsymbol{d}_i$ denote the divisor of α_i. Then it is obvious that $\boldsymbol{d}_i$ $(1 \leqq i \leqq q)$ are distinct prime divisors. Consider an element $\lambda \in \mathfrak{F}_\epsilon'$. We claim that $\boldsymbol{b}(\lambda) \neq 0$. For otherwise it follows from Corollary 3 of Lemma 28 that $\boldsymbol{b}(s\lambda) = 0$ for every $s \in W$. But since $\pi(\lambda) \neq 0$, this implies that $\boldsymbol{c}(s\lambda) = 0$ for all $s \in W$. However in view of [2(i), Lemma 37], this means that the analytic function ϕ_λ on $A_\mathfrak{p}$ must be identically zero. But this is impossible since $\phi(\lambda:1) = 1$. Hence $\boldsymbol{b}(\lambda)$ is never zero unless $\pi(\lambda) = 0$ $(\lambda \in \mathfrak{F}_\epsilon)$ and therefore $\boldsymbol{d} = k_1\boldsymbol{d}_1 + \cdots + k_q\boldsymbol{d}_q$ where $k_1, \cdots, k_q$ are certain nonnegative integers. The divisors $\boldsymbol{d}_i$ are obviously invariant under the transformation $\lambda \to -\lambda$ of $\mathfrak{F}_\epsilon$. Hence $2\boldsymbol{d}$ is the divisor of the function $\boldsymbol{b}(\lambda)\boldsymbol{b}(-\lambda)$. But then by Corollary 2 of Lemma 28, $\boldsymbol{d}$ must be invariant under W. We claim that $k_i \leqq 1$ $(1 \leqq i \leqq q)$. For otherwise suppose $k_1 \geqq 2$ and select a point $\lambda_0 \in \mathfrak{F}_R$ such that $\alpha_1(\lambda_0) = 0$ while $\alpha_i(\lambda_0) \neq 0$ $(2 \leqq i \leqq q)$. Then $\boldsymbol{c} = \boldsymbol{b}/\pi$, considered as a meromorphic function on $\mathfrak{F}_\epsilon$, is holomorphic around λ_0 and $\boldsymbol{c}(\lambda_0) = 0$. Since the divisor of $\boldsymbol{c}$ is invariant under W, it follows that $\boldsymbol{c}$ is holomorphic around $s\lambda_0$ and $\boldsymbol{c}(s\lambda_0) = 0$ for every $s \in W$. Let U be a sufficiently small compact neighborhood of λ_0 in $\mathfrak{F}_R$. We now use the notation of [2(i), § 10]. Then if N is a sufficiently large positive number, $\Phi(s\lambda:h)$ is defined for $\lambda \in U$, $s \in W$ and $h \in A_\mathfrak{p}(N)$ and it follows from [2(i), Lemma 37] that

$$e^{\rho(\log h)}\phi(\lambda:h) = \sum_{s \in W} \boldsymbol{c}(s\lambda)\Phi(s\lambda:h) \qquad (h \in A_\mathfrak{p}(N))$$

for $\lambda \in U' = U \cap \mathfrak{F}_R'$. Hence if we fix $h \in A_\mathfrak{p}(N)$ and make λ tend to λ_0 it becomes clear (see [2(i), Corollary 2 of Lemma 28]) that

$$e^{\rho(\log h)}\phi(\lambda_0:h) = \sum_{s \in W} \boldsymbol{c}(s\lambda_0)\Phi(s\lambda_0:h) = 0 \qquad (h \in A_\mathfrak{p}(N)).$$

However this is impossible because the analytic function ϕ_{λ_0} on $A_\mathfrak{p}$ is not identically zero. In fact $\phi(\lambda_0:1) = 1$. This proves that $k_i = 0$ or 1 $(1 \leqq i \leqq q)$. Hence we may assume that the divisor of $\boldsymbol{c}^{-1}$ is $\boldsymbol{d}_1 + \boldsymbol{d}_2 + \cdots + \boldsymbol{d}_p$ for some integer p $(0 \leqq p \leqq q)$. Put $\pi_0 = \alpha_1\alpha_2 \cdots \alpha_p$. $(\pi_0 = 1$ if $p = 0.)$ Since

$\boldsymbol{d}_1 + \cdots + \boldsymbol{d}_p$ is invariant under W, it is clear that $\pi_0{}^s = \epsilon_0(s)\pi_0$ $(s \in W)$ where $\epsilon_0(s) = \pm 1$. Put $\boldsymbol{b}_0 = \pi_0 \mathbf{c}$. Then the divisor of $\boldsymbol{b}_0$ is zero. Hence we have obtained the following result.

LEMMA 29. *The functions* $\boldsymbol{c}^{-1}$ *and* $\boldsymbol{b}_0 = \pi_0 \boldsymbol{c}$ *are everywhere holomorphic on* $\mathfrak{F}_\epsilon$. *Moreover* $\boldsymbol{b}_0$ *is nowhere zero on* $\mathfrak{F}_\epsilon$.

Define $\boldsymbol{b}_0'$ and π_0' in an analogous way (corresponding to $\mathfrak{m}$). Then $\boldsymbol{b}_0' = \pi_0' \boldsymbol{c}'$ and $\boldsymbol{b}_0'$, $1/\boldsymbol{b}_0'$ are both holomorphic on $\mathfrak{F}_\epsilon$. Put $\pi_1 = \pi/\pi_0$, $\pi_1' = \pi'/\pi_0'$. Then $\boldsymbol{b}_0 = \Gamma \pi_1' \boldsymbol{b}_0'/\pi_1$. But since $\boldsymbol{b}_0$ and $\boldsymbol{b}_0'$ have no zeros, it follows that $\Gamma_0 = \Gamma \pi_1'/\pi_1$ and its reciprocal are both holomorphic on $\mathfrak{F}_\epsilon$. Moreover we saw during the proof of Lemma 28 that

$$v_k(\lambda_i{}^*)\pi(\lambda)\boldsymbol{c}(\lambda_i) = {}'\Gamma_{ki}(\lambda)\pi'(\lambda_i)\boldsymbol{c}'(\lambda_i) \qquad (1 \leqq i, k \leqq r)$$

for $\lambda \in \mathfrak{F}_R'$. But $\pi(\lambda)\boldsymbol{c}(\lambda_i) = \epsilon(s_i)\boldsymbol{b}(\lambda_i) = \epsilon(s_i)\Gamma(\lambda_i)\boldsymbol{b}'(\lambda_i)$. Also $\boldsymbol{b}'(\lambda_i) \neq 0$ since $\pi(\lambda) \neq 0$ (Corollary 3 of Lemma 28). Therefore

$${}'\Gamma_{ki}(\lambda) = \epsilon(s_i)v_k(s_i\lambda^*)\Gamma(s_i\lambda) \qquad (1 \leqq i, k \leqq r)$$

and so, by analytic continuation, this relation holds for all $\lambda \in \mathfrak{F}_\epsilon$. Put $\Gamma_{ki}(\lambda) = \epsilon_0(s_i)v_k(s_i\lambda^*)\Gamma_0(s_i\lambda)$ $(1 \leqq i, k \leqq r, \lambda \in \mathfrak{F}_\epsilon)$. Then it follows from Lemma 26 and the definition of ${}'\Gamma_{ki}(\lambda)$ that

$$\pi_0(\lambda)\Theta_k(\lambda : m) = \sum_{1 \leqq i \leqq r} \Gamma_{ki}(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i : m) \qquad (m \in M)$$

for $\lambda \in \mathfrak{F}_R'$. Therefore since both sides are analytic functions of λ, this holds for all $\lambda \in \mathfrak{F}_R$.

LEMMA 30. *There exist analytic functions* Γ_{ij} $1 \leqq i, j \leqq r$ *on* $\mathfrak{F}_R$ *with the following properties.*

(1) $\pi_0(\lambda)\Theta_i(\lambda : m) = \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda)\pi_0'(s_j\lambda)\theta(s_j\lambda : m)$

$$(1 \leqq i \leqq r, \lambda \in \mathfrak{F}_R, m \in M).$$

(2) *We can find an integer* $d \geqq 0$ *such that*

$$(1 + \| \lambda \|)^{-d} \sum_{i,j} | \Gamma_{ij}(\lambda ; \partial(v)) |$$

remains bounded for any fixed $v \in S(\mathfrak{h}_{\mathfrak{p}})$ *as* λ *varies in* $\mathfrak{F}_R$.

In order to verify the second property we proceed as follows. In view of Lemma 58 of [2(i)] and the definition of Γ_{ij}, it would be enough to show that $\sup_{\lambda \in \mathfrak{F}_{\epsilon'}} (1 + \| \lambda \|)^{-d} | \Gamma_0(\lambda) | < \infty$ for some $\epsilon' > 0$ and $d \geqq 0$. Since $\Gamma_0 = \Gamma \pi_1'/\pi_1$ and Γ_0 has no zeros on $\mathfrak{F}_\epsilon$, it follows that π_1' divides π_1 in

$S(\mathfrak{h}_{\mathfrak{p}})$. Therefore by the corollary of Lemma 59 of [2(i)], it would be sufficient to verify that $\sup_{\lambda \in \mathfrak{F}_\epsilon} (1 + \|\lambda\|)^{-d} |\Gamma(\lambda)| < \infty$ for some $d \geqq 0$. But $\Gamma(\lambda) = {}'\Gamma_{11}(\lambda)$ and so this follows immediately from Lemma 23 and the definition of ${}'\Gamma_{11}$.

If we take into account Lemma 52 of [2(i)], we get the following result by a similar argument.

LEMMA 31. *We can select an integer* $d \geqq 0$ *with the following property. For any* $u \in S(\mathfrak{h}_{\mathfrak{p}})$, $\sup_{\lambda \in \mathfrak{F}_R} (1 + \|\lambda\|)^{-d} |\boldsymbol{b}_0(\lambda ; \partial(u))|$ *is finite.*

The following lemma will be needed in Section 13.

LEMMA 32. *Let* p *be an element in* $S(\mathfrak{h}_{\mathfrak{p}})$ *such that* $p^s = \epsilon_0(s)p$ $(s \in W)$. *Then* $p = \pi_0 q$ *for some* $q \in I(\mathfrak{h}_{\mathfrak{p}})$.

Fix an element $\alpha \in \Sigma$. It follows easily (see the proof of Lemma 10 of [2(i)]) that $\epsilon_0(s_\alpha) = -1$ or 1 according as α divides π_0 or not. Now suppose α divides π_0. Then $p^{s_\alpha} = -p$ and therefore α divides p. This shows that π_0 divides p in $S(\mathfrak{h}_{\mathfrak{p}})$ and our assertion is now obvious.

10. The relationship between φ and θ. Lemmas 27 and 30 give us an approximate connection between the functions ϕ and θ. Since $\mathfrak{l}$ lies in the center of $\mathfrak{m}$, it is obvious that $\theta(\lambda : m \exp H) = \exp\{\lambda^*(H) - \rho(H)\}\theta(\lambda : m)$ for $H \in \mathfrak{l}_0$, $\lambda \in \mathfrak{F}$ and $m \in M$. Therefore it follows from Lemma 30 that

$$\pi_0(\lambda) e^{\rho(H)} \Theta_i(\lambda : m \exp(H)) = \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : m) \qquad (1 \leqq i \leqq r).$$

On the other hand

$$\Phi_i(\lambda : h ; \eta : H) = e^{\rho(H)} \phi(\lambda : h \exp H ; \eta \nu_i) \qquad (1 \leqq i \leqq r)$$

for $\eta \in \mathfrak{M}$. Therefore we get the following result from the corollary of Lemma 27.

LEMMA 33. *For a given* $\eta \in \mathfrak{M}$, *we can choose an integer* $k \geqq 0$ *and a positive number* a *such that*

$$\Big| \pi_0(\lambda) e^{\rho(\log h + H)} \phi(\lambda : h \exp H ; \eta \nu_i) - \sum_{1 \leqq j \leqq r} \Gamma_{ij}(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : h ; \eta) e^{\rho(\log h)} \Big|$$
$$\leqq a(1 + \|\lambda\|)^k (1 + \|H\|)^k e^{-\beta(H)} (1 + \|\log h\|)^d \qquad (1 \leqq i \leqq r)$$

for $\lambda \in \mathfrak{F}_R, h \in A_{\mathfrak{p}}^+$ *and* $H \in \mathfrak{l}_0^+$ *provided* $\beta(H) \geqq 1$. (*Here* d *has the same meaning as in* [2(i), Theorem 3].)

Now fix an element $b \in \mathfrak{B}$ and consider the differential operators $\mu_0(b)$ and $\mu(b)$ of Lemma 10. Then $\mu(b) = \sum_{1 \leqq i \leqq s} g_i \eta_i$ where $g_i \in \mathfrak{R}_0$ and $\eta_i \in \mathfrak{M}_{\mathfrak{p}}$. From Lemma 7, we can select a positive number a_1 such that $|g_i(h \exp H)| \leqq a_1 e^{-\beta(H)}$ for $h \in A_{\mathfrak{p}}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$. Hence

$$|\phi(\lambda : h \exp H; \mu(b))| \leqq a_1 e^{-\beta(H)} \sum_{1 \leqq j \leqq s} |\phi(\lambda : h \exp H; \eta_j)|.$$

On the other hand by Lemma 46 of [2(i)], there exists an integer $k_1 \geqq 0$ and a constant $a_2 > 0$ such that

$$\sum_{1 \leqq j \leqq s} |\phi(\lambda : h \exp H; \eta_j)| \\ \leqq a_2(1 + \|\lambda\|)^{k_1}(1 + \|H\|)^d(1 + \|\log h\|)^d e^{-\rho(H + \log h)}$$

for all $\lambda \in \mathfrak{F}_R$. This shows that

$$\begin{aligned} & e^{\rho(H + \log h)} |\phi(\lambda : h \exp H; b) - \phi(\lambda : h \exp H; \mu_0(b))| \\ & = e^{\rho(H + \log h)} |\phi(\lambda : h \exp H; \mu(b))| \\ & \leqq a_1 a_2 (1 + \|\lambda\|)^{k_1} e^{-\beta(H)} (1 + \|H\|)^d (1 + \|\log h\|)^d \quad (h \in A_{\mathfrak{p}}^+, H \in \mathfrak{l}_0^+) \end{aligned}$$

provided $\beta(H) \geqq 1$. Since $\mu_0(b) \in \mathfrak{M}$ and $\nu_1 = 1$, we can now apply Lemma 33 to $\eta = \mu_0(b)$ and thus obtain the following result. Put $\Gamma_j(\lambda) = \Gamma_{1j}(\lambda)$ $(1 \leqq j \leqq r)$.

LEMMA 34. *For any $b \in \mathfrak{B}$, we can choose an integer $k \geqq 0$ and a positive number a such that*

$$\begin{aligned} & |\pi_0(\lambda) e^{\rho(\log h + H)} \phi(\lambda : h \exp H; b) \\ & \qquad - \sum_{1 \leqq j \leqq r} \Gamma_j(\lambda) e^{\lambda_j^*(H)} \pi_0'(\lambda_j) \theta(\lambda_j : h; \mu_0(b)) e^{\rho(\log h)}| \\ & \qquad \leqq a(1 + \|\lambda\|)^k (1 + \|H\|)^k e^{-\beta(H)} (1 + \|\log h\|)^d \end{aligned}$$

for $\lambda \in \mathfrak{F}_R$, $h \in A_{\mathfrak{p}}^+$ and $H \in \mathfrak{l}_0^+$ provided $\beta(H) \geqq 1$.

We recall that the element H_0 of Section 2 has been kept fixed throughout our discussion. It is obvious that $\rho(H_0) > 0$. Select a number ϵ such that $0 < \epsilon < 1$ and let U be the set of all points $H \in \mathfrak{h}_{\mathfrak{p}_0}$ which satisfy the conditions $\alpha(H) \geqq (1 - \epsilon)\alpha(H_0)$ $(\alpha \in P)$ and $\|H\| \leqq (1 + \epsilon)\|H_0\|$. Then U is a neighborhood of H_0 in $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$. Put $H_\epsilon = H - (1 - \epsilon)H_0$ for $H \in U$. Then $H_\epsilon \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ and $\exp tH = \exp t(1 - \epsilon)H_0 \exp tH_\epsilon$ $(t \in R)$. Hence if $t \geqq t_0 = \{(1 - \epsilon)\beta(H_0)\}^{-1}$, it follows from Lemma 34 that

$$\begin{aligned} & |\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH; b) \\ & \qquad - \sum_{1 \leqq i \leqq r} \Gamma_i(\lambda) \exp\{t(1 - \epsilon)\lambda_i^*(H_0)\} \pi_0'(\lambda_i) \theta(\lambda_i : \exp tH_\epsilon; \mu_0(b)) e^{t\rho(H_\epsilon)}| \\ & \qquad \leqq a(1 + \|\lambda\|)^k (1 + \|tH_0\|)^k (1 + \|tH_\epsilon\|)^d e^{-t/t_0} \end{aligned}$$

for $H \in U$ and $\lambda \in \mathfrak{F}_R$. Moreover since H_0 lies in the center of $\mathfrak{m}$, it is clear that

$$\theta(\lambda_i : \exp tH ; \mu_0(b)) \\ = \exp\{t(1-\epsilon)\lambda_i^*(H_0) - t(1-\epsilon)\rho(H)\}\theta(\lambda_i : \exp tH_\epsilon ; \mu_0(b)).$$

Also $\| H_\epsilon \| \leqq \| H \| + (1-\epsilon) \| H_0 \| \leqq 2 \| H_0 \|$. Therefore if we put $a_1 = 2^d(1 + \| H_0 \|)^{k+d} a$, it follows that

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b) - \sum_i \Gamma_i(\lambda) \pi_0'(\lambda_i) e^{t\rho(H)} \theta(\lambda_i : \exp tH ; \mu_0(b))| \\ \leqq a_1(1 + \| \lambda \|)^k (1+t)^{k+d} e^{-t/t_0}$$

for $H \in U$, $\lambda \in \mathfrak{F}_R$ and $t \geqq t_0$. On the other hand by applying Lemma 46 and Theorem 3 of [2(i)] both to $\phi(\lambda : \exp tH ; b)$ and $\theta(\lambda_i : \exp tH ; \mu_0(b))$ and making use of the second statement of Lemma 30, we conclude that

$$|\pi_0(\lambda)\phi(\lambda : h ; b)| + \sum_i |\Gamma_i(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i : h ; \mu_0(b))| \\ \leqq a_2(1 + \| \lambda \|)^{k_2} e^{-\rho(\log h)} (1 + \| \log h \|)^{d_2}$$

for suitable constants $a_2, k_2, d_2 \geqq 0$ and $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$, $\lambda \in \mathfrak{F}_R$. Since $\lim_{t \to +\infty} t^q e^{-t/2t_0} = 0$ for any $q \geqq 0$, we thus obtain the following result.

LEMMA 35. *There exists a neighborhood U of H_0 in $\mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ and a positive number t_0 with the following property. If b is any given element in $\mathfrak{B}$, we can select an integer $k \geqq 0$ and a constant $a > 0$ such that*

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b) - \sum_i \Gamma_i(\lambda) \pi_0'(\lambda_i) e^{t\rho(H)} \theta(\lambda_i : \exp tH ; \mu_0(b))| \\ \leqq a(1 + \| \lambda \|)^k e^{-t/2t_0}$$

for $H \in U$, $\lambda \in \mathfrak{F}_R$ and $t \geqq 0$.

11. Proof of Theorem 1. We shall now deduce an important result from Lemma 35.

THEOREM 1. *For any $b \in \mathfrak{B}$, we can choose an integer $k \geqq 0$ such that $(1 + \| \lambda \|)^{-k} |\pi_0(\lambda)\phi(\lambda : h ; b) e^{\rho(\log h)}|$ remains bounded as λ and h vary in $\mathfrak{F}_R$ and $\mathrm{Cl}(A_{\mathfrak{p}}^+)$ respectively.*

We shall prove this theorem by induction on $\dim_R \mathfrak{g}_0$. Let S_+ be the set of all points $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}^+)$ with $\| H \| = 1$. Then S_+ is compact. Therefore it is obviously sufficient to prove the following lemma.

LEMMA 36. *For a given $b \in \mathfrak{B}$ and $H_0 \in S_+$, we can choose a neighborhood V of H_0 in S_+, an integer $k_1 \geqq 0$ and a positive number a_1 such that*

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b)| \leqq a_1(1 + \|\lambda\|)^{k_1}$$

for $\lambda \in \mathfrak{F}_R$, $H \in V$ and $t \geqq 0$.

We now construct $\mathfrak{m}_0$ corresponding to this H_0 and use the notation of Lemma 35. Since $\mathfrak{m}_0$ is reductive, its derived algebra $\mathfrak{m}_0' = [\mathfrak{m}_0, \mathfrak{m}_0]$ is semisimple and $\dim_R \mathfrak{m}_0' < \dim_R \mathfrak{g}_0$ because H_0 lies in the center of $\mathfrak{m}_0$. Therefore our induction hypothesis is applicable to $\mathfrak{m}_0'$. Define σ as in Lemma 12 and put

$$\theta'(\lambda : m) = \int_{M_K} \exp\{\lambda^*(H(mk')) - \sigma(H(mk'))\} dk' \qquad (\lambda \in \mathfrak{F}_R, m \in M),$$

where dk' denotes, as before, the normalized Haar measure of M_K. Now $\mathfrak{l}_0$ lies in the center of $\mathfrak{m}_0$ and $\mathfrak{m}_0 = \mathfrak{l}_0 + \mathfrak{m}_0' + \mathfrak{m}_{\mathfrak{k}_0}$. Hence by applying the induction hypothesis to $\mathfrak{m}_0'$, it is easily seen that for any $\eta \in \mathfrak{M}$, we can select an integer $k_2 \geqq 0$ and a positive number a_2 such that

$$|\pi_0'(\lambda) e^{\sigma(H)} \theta'(\lambda : \exp H ; \eta)| \leqq a_2(1 + \|\lambda\|)^{k_2}$$

for all $\lambda \in \mathfrak{F}_R$ and $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. Also it is obvious that

$$\theta(\lambda : h) = \exp(\sigma(\log h) - \rho(\log h)) \theta'(\lambda : h)$$

for $h \in A_{\mathfrak{p}}$. Let $\mu_0(b)'$ denote the image of $\mu_0(b)$ under the automorphism of $\mathfrak{M}$ over C which leaves every element of $\mathfrak{m}_0' + \mathfrak{m}_{\mathfrak{k}_0}$ fixed and maps H on $H - \rho(H)$ for $H \in \mathfrak{l}$. Then clearly

$$\theta(\lambda : h ; \mu_0(b)) = \exp(\sigma(\log h) - \rho(\log h)) \theta'(\lambda : h ; \mu_0(b)')$$

and therefore if we take $\eta = \mu_0(b)'$, it follows that

$$|\pi_0'(\lambda) e^{\rho(H)} \theta(\lambda : \exp H ; \mu_0(b))| \leqq a_2(1 + \|\lambda\|)^{k_2}$$

for $\lambda \in \mathfrak{F}_R$ and $H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+)$. But then from the second statement of Lemma 30, we can conclude that

$$|\sum_i \pi_0'(\lambda_i) \Gamma_i(\lambda) e^{\rho(H)} \theta(\lambda_i : \exp H ; \mu_0(b))| \leqq a_3(1 + \|\lambda\|)^{k_3}$$
$$(\lambda \in \mathfrak{F}_R, H \in \mathrm{Cl}(\mathfrak{h}_{\mathfrak{p}_0}{}^+))$$

for suitable constants $a_3, k_3 \geqq 0$. Hence it follows from Lemma 35 that we can choose constants $a_1, k_1 \geqq 0$ and a neighborhood V of H_0 in S_+ such that

$$|\pi_0(\lambda) e^{t\rho(H)} \phi(\lambda : \exp tH ; b)| \leqq a_1(1 + \|\lambda\|)^{k_1}$$

for $H \in V$, $\lambda \in \mathfrak{F}_R$ and $t \geqq 0$. This proves Lemma 36 and hence also Theorem 1.

12. The space $I(G)$. Let x be an element in G. Then x can be written uniquely (see [2(f), Lemma 31]) in the form $k \exp X$ $(k \in K, X \in \mathfrak{p}_0)$. Put $D(x) = \{\det(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{p}}\}^{\frac{1}{2}}$, where $(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{p}}$ denotes the restriction on $\mathfrak{p}$ of the linear transformation

$$\sinh \operatorname{ad} X/\operatorname{ad} X = \sum_{q \geqq 0} (\operatorname{ad} X)^{2q}/(2q+1)\,!$$

of $\mathfrak{g}$. Then D is an analytic function on G which is obviously spherical. Put[10] $D_q(x) = (1 + \| \log | x | \|)^q D(x)$.

Definition. *Let $I(G)$ denote the set of all complex-valued functions ϕ on G of class C^∞ satisfying the following two conditions:*

(1) *ϕ is spherical.*

(2) *For any $b \in \mathfrak{B}$ and any integer $q \geqq 0$,*

$$\sup_{x \in G} D_q(x) | \phi(x;b) | < \infty.$$

Put $\tau_{b,q}(\phi) = \sup D_q(x) | \phi(x;b) |$. Then $\tau_{b,q}$ is a seminorm on $I(G)$ and the collection of these seminorms, for all $b \in \mathfrak{B}$ and $q \geqq 0$, defines a topology on $I(G)$ in the usual way so that $I(G)$ becomes a locally convex space.

We note that $(e^t - e^{-t})/2t = \sum_{q \geqq 0} t^{2q}/(2q+1)\,!$ is an increasing function of t for $t \geqq 0$. Hence it follows easily that $D(x) \geqq D(1) = 1$ $(x \in G)$. Moreover $(1 - e^{-2t})/2t$ remains bounded for $t \geqq 0$ and therefore $D(h) e^{-\rho(\log h)}$ also remains bounded as h varies in $\mathrm{Cl}(A_{\mathfrak{p}}^+)$. We shall need these facts presently.

Theorem 2. *For any $b \in \mathfrak{B}$, we can select an integer $q \geqq 0$ and a constant $c > 0$ such that*

$$D(x) | \pi_0(\lambda) \phi(\lambda : x ; b) | \leqq c(1 + \| \lambda \|)^q$$

for all $x \in G$ and $\lambda \in \mathfrak{F}_R$.

Obviously we can choose a finite number of elements $b_1, \cdots, b_r \in \mathfrak{B}$ and analytic functions $a_1, \cdots, a_r$ on K such that $b^k = \sum_{1 \leqq i \leqq r} a_i(k) b_i$ for $k \in K$. Now suppose $h \in \mathrm{Cl}(A_{\mathfrak{p}}^+)$ and $k \in K$. Then

$$\phi(\lambda : hk ; b) = \phi(\lambda : h ; b^k) = \sum_i a_i(k) \phi(\lambda : h ; b_i)$$

and therefore

$$| \phi(\lambda : hk ; b) | \leqq a \sum_i | \phi(\lambda : h ; b_i) |$$

where $a = \sup_{k \in K} (| a_1(k) |, \cdots, | a_r(k) |)$. On the other hand $D(hk) = D(h)$

and $D(h)e^{-\rho(\log h)}$ remains bounded as h varies in $\mathrm{Cl}(A_{\mathfrak{p}}^{+})$. Therefore by Theorem 1, we can choose an integer $q \geqq 0$ and a constant $c > 0$ such that

$$D(h)\,|\,\pi_0(\lambda)\phi(\lambda : hk; b)\,| \leqq c(1 + \|\lambda\|)^q$$

for all $\lambda \in \mathfrak{F}_R$, $h \in \mathrm{Cl}(A_{\mathfrak{p}}^{+})$ and $k \in K$. But $G = K(\mathrm{Cl}(A_{\mathfrak{p}}^{+}))K$ (see [2(f), § 12]) and D and ϕ_λ are spherical functions. Hence it is clear that

$$D(x)\,|\,\pi_0(\lambda)\phi(\lambda : x; b)\,| \leqq c(1 + \|\lambda\|)^q$$

for $x \in G$ and $\lambda \in \mathfrak{F}_R$. This proves the theorem.

Now $\mathfrak{F}_R$ being a real Euclidean space, we can define the locally convex space $\mathcal{C}(\mathfrak{F}_R)$ as usual (see [2(g), § 2]). It consists of all complex-valued C^∞ functions a on $\mathfrak{F}_R$ such that $\sup_{\lambda \in \mathfrak{F}_R} (1 + \|\lambda\|)^q\,|\,a(\lambda; \partial(p)\,| < \infty$ for $p \in S(\mathfrak{h}_{\mathfrak{p}})$ and any integer $q \geqq 0$. Let $d\lambda$ denote the Euclidean measure on $\mathfrak{F}_R$. Then if $a \in \mathcal{C}(\mathfrak{F}_R)$, it follows from Theorem 2 that the integral

$$\int_{\mathfrak{F}_R} |\,\pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\,|\, d\lambda \qquad (b \in \mathfrak{B})$$

converges uniformly with respect to $x \in G$. This shows that

$$\phi_a(x) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x)\, d\lambda \qquad (x \in G)$$

is a C^∞ function on G and

$$\phi_a(x; b) = \int \pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\, d\lambda \qquad (b \in \mathfrak{B}).$$

THEOREM 3. *For any* $a \in \mathcal{C}(\mathfrak{F}_R)$, *put*

$$\phi_a(x) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x)\, d\lambda \qquad (x \in G).$$

Then $\phi_a \in I(G)$ *and* $a \rightarrow \phi_a$ *is a continuous mapping of* $\mathcal{C}(\mathfrak{F}_R)$ *into* $I(G)$. *Also*

$$\phi_a(x; b) = \int_{\mathfrak{F}_R} \pi_0(\lambda)a(\lambda)\phi(\lambda : x; b)\, d\lambda \qquad (x \in G, b \in \mathfrak{B}).$$

It is obvious from its definition that ϕ_a is spherical. Moreover if $x = k_1 h k_2$ $(k_1, k_2 \in K; h \in \mathrm{Cl}(A_{\mathfrak{p}}^{+}))$, it is clear that

$$D_r(x)\phi_a(x; b) = D_r(h)\phi_a(h; b^{k_2})$$

for $b \in \mathfrak{B}$ and any integer $r \geqq 0$. Let $\mathfrak{D}(\mathfrak{h}_{\mathfrak{p}})$ denote the algebra of polynomial differential operators on $\mathfrak{h}_{\mathfrak{p}}$ (see [2(g), § 2]). Then as we saw during the proof of Theorem 2, it would be sufficient to prove the following lemma.

LEMMA 37. *Let b be an element in $\mathfrak{B}$ and s an integer $\geqq 0$. Then we can select a finite number of elements $d_0, d_1, \cdots, d_N$ in $\mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that*

$$(1+\|\log h\|)^s e^{\rho(\log h)} |\phi_a(h;b)| \leqq \sum_{0\leqq i\leqq N} \sup_{\lambda\in\mathfrak{F}_R} |a(\lambda;d_i)|$$

for $a \in \mathscr{C}(\mathfrak{F}_R)$ and $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$.

We shall use induction on $\dim \mathfrak{h}_\mathfrak{p}$. The case $\mathfrak{h}_\mathfrak{p} = \{0\}$ is obviously trivial. So let us assume that $\dim \mathfrak{h}_\mathfrak{p} \geqq 1$. Define S_+ as in Section 11. Since S_+ is compact, it would be enough to prove the following statement.

LEMMA 38. *Fix b and s as above. Then for a given $H_0 \in S_+$, we can select a neighborhood V of H_0 in S_+ and a finite number of elements $d_0, \cdots, d_N \in \mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that*

$$(1+t)^s e^{t\rho(H)} |\phi_a(\exp tH;b)| \leqq \sum_{0\leqq i\leqq N} \sup_{\lambda\in\mathfrak{F}_R} |a(\lambda;d_i)|$$

for $a \in \mathscr{C}(\mathfrak{F}_R)$, $H \in V$ and $t \geqq 0$.

We use the notation of Lemma 35 (corresponding to the element H_0 selected above). Then by this lemma, we can choose a neighborhood V of H_0 in S_+, an integer $k \geqq 0$ and two constants c, $t_0 > 0$ such that

$$\begin{aligned}|\pi_0(\lambda) e^{t\rho(H)}\phi(\lambda:\exp tH;b) - \sum_{1\leqq i\leqq r} \Gamma_i(\lambda)\pi_0'(\lambda_i)\theta(\lambda_i:\exp tH;\mu_0(b))e^{t\rho(H)}| \\ \leqq c(1+\|\lambda\|)^k e^{-t/t_0}\end{aligned}$$

for $H \in V$, $\lambda \in \mathfrak{F}_R$ and $t \geqq 0$. Put

$$f_a(m) = \int_{\mathfrak{F}_R} \pi_0'(\lambda)a(\lambda)\theta(\lambda:m)\,d\lambda \qquad (m \in M, a \in \mathscr{C}(\mathfrak{F}_R)).$$

Then by induction hypothesis, Lemma 37 is applicable to $\mathfrak{m}_0' = [\mathfrak{m}_c, \mathfrak{m}_0]$ instead of $\mathfrak{g}_0$ and so it follows easily that we can choose a finite number of elements $d_1', \cdots, d_p' \in \mathfrak{D}(\mathfrak{h}_\mathfrak{p})$ such that

$$(1+\|\log h\|)^s e^{\rho(\log h)} |f_a(h;\mu_0(b))| \leqq \sum_{1\leqq i\leqq p} \sup_{\lambda\in\mathfrak{F}_R} |a(\lambda;d_i')|$$

for $a \in \mathscr{C}(\mathfrak{F}_R)$ and $h \in \mathrm{Cl}(A_\mathfrak{p}^+)$. Now put $a_i(\lambda) = \Gamma_i(s_i^{-1}\lambda)a(s_i^{-1}\lambda)$ $(1 \leqq i \leqq r)$ for $a \in \mathscr{C}(\mathfrak{F}_R)$ and $\lambda \in \mathfrak{F}_R$. Then it follows from the second statement of Lemma 30 that a_i are also in $\mathscr{C}(\mathfrak{F}_R)$. Moreover in view of the inequality stated above, it is obvious that

$$\begin{aligned}&|e^{t\rho(H)}\phi_a(\exp tH;b) \\ &\quad - \sum_{1\leqq i\leqq r} f_{a_i}(\exp tH;\mu_0(b))e^{t\rho(H)}| \leqq ce^{-t/t_0}\int (1+\|\lambda\|)^k |a(\lambda)|\,d\lambda\end{aligned}$$

for $H \in V$ and $t \geqq 0$. On the other hand we can choose $d_0 \in S(\mathfrak{h}_{\mathfrak{p}})$ such that

$$c(1+t)^s e^{-t/t_0} \int (1+\|\lambda\|)^k |a(\lambda)| \, d\lambda \leqq \sup_{\lambda \in \mathfrak{F}_R} |d_0(\lambda) a(\lambda)|$$

for $t \geqq 0$ and $a \in \mathcal{B}(\mathfrak{F}_R)$. Furthermore

$$(1+t)^s e^{t\rho(H)} |f_{a_i}(\exp tH; \mu_0(b))| \leqq \sum_{1 \leqq j \leqq p} \sup_{\lambda \in \mathfrak{F}_R} |a(\lambda; d_j')|$$

for $H \in V$ and $t \geqq 0$ and, in view of the second statement of Lemma 30, we can select $d_1, \cdots, d_N \in \mathfrak{D}(\mathfrak{h}_{\mathfrak{p}})$ such that

$$\sum_{1 \leqq i \leqq r} \sum_{1 \leqq j \leqq p} \sup_{\lambda \in \mathfrak{F}_R} |a_i(\lambda; d_j')| \leqq \sum_{1 \leqq i \leqq N} \sup_{\lambda \in \mathfrak{F}_R} |a(\lambda; d_i)|$$

for $a \in \mathcal{B}(\mathfrak{F}_R)$. Therefore the assertion of Lemma 38 is now obvious. This completes the proof of Theorem 3.

13. The distribution T_μ.

Let dx denote the Haar measure on G.

LEMMA 39. *Fix an element* μ *in* $\mathfrak{F}_R$. *Then for any* $a \in \mathcal{B}(\mathfrak{F}_R)$, *the integral*

$$\int_G (\operatorname{conj} \phi(\mu : x)) \phi_a(x) \, dx$$

is well defined and the mapping

$$T_\mu \colon a \to \int (\operatorname{conj} \phi(\mu : x)) \phi_a(x) \, dx \qquad (a \in \mathcal{B}(\mathfrak{F}_R))$$

is a $\mathcal{B}$*-distribution on* $\mathfrak{F}_R$.

This is an immediate consequence of Theorem 3 and the following result.

LEMMA 40. *Let* $f \in I(G)$, $\mu \in \mathfrak{F}_R$ *and* $b_1, b_2 \in \mathfrak{B}$. *Then the integral*

$$\int_G |\phi(\mu : xy; b_1) f(x; b_2)| \, dx \qquad (y \in G)$$

converges uniformly with respect to y *on every compact subset of* G. *Moreover the mapping*

$$f \to \int_G |\phi(\mu : x; b_1) f(x; b_2)| \, dx \qquad (f \in I(G))$$

is continuous on $I(G)$.

From Lemma 46 of [2(i)] we can select a positive number c_1 such that $|\phi(\mu : x; b_1)| \leqq c_1 \phi(0 : x)$ for $x \in G$. Moreover if Ω is a compact subset of G, there exists a positive number c_2 such that $\phi(0 : xy) \leqq c_2 \phi(0 : x)$ for

$x \in G$ and $y \in \Omega$ (see [2(i), Lemma 48]). Therefore it would be sufficient to prove that

$$\int |\phi(0:x)f(x;b_2)|\, dx < \infty$$

and the mapping

$$f \to \int |\phi(0:x)f(x;b_2)|\, dx \qquad (f \in I(G))$$

is continuous on $I(G)$. Put $\Delta(\exp H) = \prod_{\alpha \in P_+} (e^{\alpha(H)} - e^{-\alpha(H)})$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$ as in [2(i), § 5]. Then if the Haar measure dh on $A_{\mathfrak{p}}$ is suitably normalized, we have

$$\int g(x)\, dx = \int_{A_{\mathfrak{p}}^+} \Delta(h)\, dh \int_{K \times K} g(k_1 h k_2)\, dk_1 dk_2$$

for any $g \in C_c(G)$ (see [2(f), § 12]). Therefore

$$\int |\phi(0:x)f(x;b_2)|\, dx = \int_{A_{\mathfrak{p}}^+} \Delta(h)\phi(0:h)\, dh \int_K |f(h;b_2^k)|\, dk.$$

We can obviously select a finite number of linearly independent elements $b_3, \cdots, b_N$ in $\mathfrak{B}$ and analytic functions $g_3, \cdots, g_N$ on K such that $b_2^k = \sum_{3 \leqq i \leqq N} g_i(k) b_i$ $(k \in K)$. Then

$$|f(h;b_2^k)| \leqq \sum_{3 \leqq i \leqq N} |g_i(k)|\, |f(h;b_i)|.$$

Since K is compact, the g_i remain bounded on K and so it would be sufficient to verify that for any $b \in \mathfrak{B}$,

$$\int_{A_{\mathfrak{p}}^+} \Delta(h)\phi(0:\, h)\, |f(h;b)|\, dh < \infty$$

and the mapping

$$f \to \int_{A_{\mathfrak{p}}^+} \Delta(h)\phi(0:h)\, |f(h;b)|\, dh \qquad (f \in I(G))$$

is continuous on $I(G)$. Choose an integer $q_1 \geqq 0$ such that

$$\int_{A_{\mathfrak{p}}} (1 + \|\log h\|)^{-q_1}\, dh < \infty$$

Since $|\Delta(h)|^{\frac{1}{2}} e^{-\rho(\log h)}$ obviously remains bounded for $h \in A_{\mathfrak{p}}^+$, we can, from Theorem 3 of [2(i)], select an integer $q_2 \geqq 0$ such that

$$(1 + \|\log h\|)^{-q_2}\, |\Delta(h)|^{\frac{1}{2}} \phi(0:h)$$

is bounded on $A_{\mathfrak{p}}^+$. On the other hand it follows from the definition of D that $|\Delta(h)|^{\frac{1}{2}}(1+\|\log h\|)^{-q_3}D(h)^{-1}$ remains bounded on $A_{\mathfrak{p}}$ for a suitable integer $q_3 \geqq 0$. Hence there exists a positive number c such that $\Delta(h)\phi(0:h) \leqq cD_{q_2+q_3}(h)$ for $h \in A_{\mathfrak{p}}^{+}$. Therefore if we put $q = q_1 + q_2 + q_3$, it is clear that

$$\int_{A_{\mathfrak{p}}^{+}} \Delta(h)\phi(0:h)\,|f(h;b)|\,dh \leqq c\tau_{b,q}(f) \int_{A_{\mathfrak{p}}} (1+\|\log h\|)^{-q_1}\,dh$$

in the notation of Section 12. This proves our assertion.

COROLLARY 1. *Let Ω be a compact subset of $G \times G$. Then if $f \in I(G)$, the integral $\int_G |\phi(\mu:xy;b_1)f(xz;b_2)|\,dx$ converges uniformly for $(y,z) \in \Omega$.*

Without loss of generality we may assume that $\Omega = \omega_1 \times \omega_2$ where ω_1, ω_2 are compact subsets of G. Let ω be the image of Ω in G under the mapping $(y,z) \to z^{-1}y$. Then ω is also compact. Given any $\epsilon > 0$ we can, by Lemma 40, select a compact set V in G such that

$$\int_{{}^cV} |\phi(\mu:xy;b_1)f(x;b_2)|\,dx < \epsilon$$

for $y \in \omega$. (As usual ${}^cV$ denotes the complement of V in G.) Put $U = V\omega_2^{-1}$. Then U is also compact and ${}^cUz \subset {}^cV$ for $z \in \omega_2$. Hence if $y \in \omega_1$ and $z \in \omega_2$, it is clear that

$$\int_{{}^cU} |\phi(\mu:xy;b_1)f(xz;b_2)|\,dx = \int_{{}^cUz} |\phi(\mu:xz^{-1}y;b_1)f(x;b_2)|\,dx < \epsilon$$

from the right-invariance of the measure dx. This proves the corollary.

Now put

$$F(y:z) = \int_G \{\operatorname{conj}\phi(\mu:xy)\}f(xz)\,dx \qquad (y,z \in G).$$

Then the above corollary implies that F is a C^∞-function on $G \times G$ and

$$F(y;b_1:z;b_2) = \int_G (\operatorname{conj}\phi(\mu:xy;b_1))f(xz;b_2)\,dx$$

for $b_1, b_2 \in \mathfrak{B}$. On the other hand $F(y;b_1:z;b_2) = F(z^{-1}y;b_1:1;b_2)$ by the right-invariance of dx. Hence if we put $y = 1$ and $z = \exp tX$ $(X \in \mathfrak{g}_0, t \in R)$ and differentiate with respect to t at $t = 0$, we get $F(1;b_1:1;Xb_2) = -F(1;Xb_1:1;b_2)$. Let $b \to b^*$ denote the anti-automorphism of $\mathfrak{B}$ over R such that $(X + (-1)^{\frac{1}{2}}Y)^* = -X + (-1)^{\frac{1}{2}}Y$ $(X, Y \in \mathfrak{g}_0)$. Then the above result obviously implies the following corollary.

COROLLARY 2. *For any $b \in \mathfrak{B}$, $f \in I(G)$ and $\mu \in \mathfrak{F}_R$,*

$$\int_G (\operatorname{conj}\phi(\mu:x))f(x;b)\,dx = \int_G (\operatorname{conj}\phi(\mu:x;b^*))f(x)\,dx.$$

that

$$\int_G \phi_\lambda(x) f(x)\,dx = \int_G f(x)\exp\{(-1)^{\frac{1}{2}}\lambda(H(x)) - \rho(H(x))\}\,dx$$
$$= \int_{A_\mathfrak{p}} \exp\{(-1)^{\frac{1}{2}}\lambda(\log h) + \rho(\log h)\}\,dh \int_N f(hn)\,dn$$
$$= \int_{A_\mathfrak{p}} F_f(h)\exp\{(-1)^{\frac{1}{2}}\lambda(\log h)\}\,dh.$$

Let us now assume that $d\lambda$ is the *regular* Euclidean measure (see [2(g), § 2]) on $\mathfrak{F}_R$ and the Haar measure dh on $A_\mathfrak{p}$ is so normalized that

$$\int_{A_\mathfrak{p}} dh \int_{\mathfrak{F}_R} a(\lambda)\exp\{(-1)^{\frac{1}{2}}\lambda(\log h)\}\,d\lambda = a(0)$$

for any $a \in \mathscr{C}(\mathfrak{F}_R)$. In view of the relation $dx = e^{2\rho(\log h)}dk\,dh\,dn$, this fixes the normalization of dx as well. We shall call these the regular normalizations of $d\lambda$, dx and dh. Define $\boldsymbol{\beta}$ as in the corollary of Lemma 41.

COROLLARY. *Let a be any element in $\mathscr{C}(\mathfrak{F}_R)$. Then*

$$e^{\rho(H)} \int_{\bar{N}} \phi_a(\bar{n}\exp H)\,d\bar{n} = \int_{\mathfrak{F}_R} \boldsymbol{\beta}(\lambda)\{\pi_0(\lambda)^{-1} \sum_{s\in W} \epsilon_0(s)a(s\lambda)\}e^{(-1)^{\frac{1}{2}}\lambda(H)}\,d\lambda$$

for $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

Put $f = \phi_a$. Then from Theorem 3, f lies in $I(G)$ and therefore by Lemma 43,

$$\int F_f(h)\exp\{-(-1)^{\frac{1}{2}}\lambda(\log h)\}\,dh = \int \phi_a(x)\,\mathrm{conj}\,\phi_\lambda(x)\,dx \quad (\lambda \in \mathfrak{F}_R).$$

Now apply the corollary of Lemma 41. Then

$$\pi_0(\lambda)\int F_f(h)\exp\{-(-1)^{\frac{1}{2}}\lambda(\log h)\}\,dh = \boldsymbol{\beta}(\lambda)\sum_{s\in W}\epsilon_0(s)a(s\lambda).$$

Therefore our assertion follows immediately by the Fourier inversion formula.

We shall see in the next section that the above relation also holds if $\boldsymbol{\beta}(\lambda)$ is replaced by $|\boldsymbol{b}_0(\lambda)|^2$. This would prove that $\boldsymbol{\beta}(\lambda) = |\boldsymbol{b}_0(\lambda)|^2$ for $\lambda \in \mathfrak{F}_R$.

15. Determination of the function $\boldsymbol{\beta}$. Extend θ to an automorphism of $\mathfrak{B}$ and put $\mathfrak{N} = \theta(\bar{\mathfrak{N}})$, $\mathfrak{N}_1 = \theta(\bar{\mathfrak{N}}_1)$ and $\gamma'(q) = e^{-\rho}\gamma(q) \circ e^{\rho}$ $(q \in I_\mathfrak{g})$. Also define $\mathfrak{B}_d$ as in Lemma 9.

LEMMA 44. *Let q be an element in $I_\mathfrak{g}$ and let d denote the degree of $\gamma(q)$. Then $q - \gamma'(q) \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d$.*

Define $\mathfrak{P}$ as in Lemma 19 of [2(i)]. Then we have seen in [2(i), § 4] that $I_\mathfrak{g} = I_\mathfrak{g} \cap \mathfrak{P} + I_\mathfrak{g} \cap (\mathfrak{k}\mathfrak{B})$. On the other hand $I_\mathfrak{g} \cap (\mathfrak{k}\mathfrak{B}) = I_\mathfrak{g} \cap (\mathfrak{B}\mathfrak{k})$ is the kernel of γ (see [2(i), Theorem 1]). So it would be sufficient to consider the case when $q \in I_\mathfrak{g} \cap \mathfrak{P}$. But then it follows from [2(i), Lemma 20] that q itself is of degree d. Now $\mathfrak{g}$ is the direct sum of $\mathfrak{k}$, $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{n}$. Hence $\mathfrak{B}_d \subset \mathfrak{k}\mathfrak{B} + (\mathfrak{H}_\mathfrak{p}\mathfrak{N}) \cap \mathfrak{B}_d$ from [2(b), Lemma 12]. Therefore it follows from the definition of γ (see [2(i), § 4]) that $q - \gamma'(q) \in \mathfrak{k}\mathfrak{B} + (\mathfrak{H}_\mathfrak{p}\mathfrak{N}_1) \cap \mathfrak{B}_d$. Let $b \to b^\dagger$ $(b \in \mathfrak{B})$ denote the anti-automorphism of $\mathfrak{B}$ such that $X^\dagger = -\theta(X)$ $(X \in \mathfrak{g})$. It is clear that every element of $\mathfrak{p}$ (and therefore also of $\mathfrak{P}$) is left fixed by this anti-automorphism. Hence

$$q - \gamma'(q) = (q - \gamma'(q))^\dagger \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d.$$

This proves the lemma.

Select $u_1 = 1, u_2, \cdots, u_w \in \mathfrak{H}_\mathfrak{p}$ as in the corollary of Lemma 8 of [2(i)] and let $u \to u'$ denote the automorphism of $\mathfrak{H}_\mathfrak{p}$ given by $u' = e^{-\rho}u \circ e^{\rho}$ $(u \in \mathfrak{H}_\mathfrak{p})$.

LEMMA 45. *Suppose* $u = \sum_{1 \leqq i \leqq w} u_i\gamma(q_i)$ $(q_i \in I_\mathfrak{g})$. *Then we can choose a finite number of elements* $q_{ki} \in I_\mathfrak{g}$ *and* $\eta_{ki} \in \bar{\mathfrak{N}}_1$ $(1 \leqq k \leqq r,\ 1 \leqq i \leqq w)$ *such that*

$$u' \equiv \sum_{1 \leqq i \leqq w} u_i' q_i + \sum_{1 \leqq k \leqq r} \sum_{1 \leqq i \leqq w} \eta_{ki} u_i' q_{ki} \bmod \mathfrak{B}\mathfrak{k}.$$

We shall use induction on the degree d of u. Obviously we may assume that u is homogeneous and $d \geqq 1$. Then $u_i\gamma(q_i)$ $(1 \leqq i \leqq w)$ are also homogeneous of degree d (see the corollary of Lemma 8 of [2(i)]) and it follows from Lemma 44 that

$$\sum_i u_i' q_i - \sum_i u_i' \gamma'(q_i) \in \mathfrak{B}\mathfrak{k} + (\bar{\mathfrak{N}}_1\mathfrak{H}_\mathfrak{p}) \cap \mathfrak{B}_d.$$

But this implies that

$$u' \equiv \sum_i u_i' q_i + \sum_{1 \leqq k \leqq s} \eta_k v_k' \bmod \mathfrak{B}\mathfrak{k}$$

where $\eta_k \in \bar{\mathfrak{N}}_1$ and $v_k \in \mathfrak{H}_\mathfrak{p} \cap \mathfrak{B}_{d-1}$ $(1 \leqq k \leqq s)$. On the other hand $\mathfrak{H}_\mathfrak{p} = \sum_{1 \leqq i \leqq w} J u_i$ where $J = I(\mathfrak{h}_\mathfrak{p}) = \gamma(I_\mathfrak{g})$. Therefore our assertion follows by applying the induction hypothesis to v_k.

Select $\alpha_1, \cdots, \alpha_l \in \Sigma$ as in [2(i), § 3] and consider the additive group L generated by Σ. Then $(\alpha_1, \cdots, \alpha_l)$ is a set of independent generators of L. We say that an element $b \in \mathfrak{B}$ is of rank β $(\beta \in L)$ if $[H, b] = Hb - bH = \beta(H)b$ for every $H \in \mathfrak{h}_\mathfrak{p}$. Let L_+ be the set of all elements $\beta \in L$ of the form $\beta = m_1\alpha_1 + \cdots + m_l\alpha_l$ where $m_1, \cdots, m_l$ are nonnegative integers which are not all zero. Let $(\bar{\mathfrak{N}}_1)_{-\beta}$ $(\beta \in L_+)$ denote the set of all elements in $\bar{\mathfrak{N}}_1$ of rank $-\beta$. Then it is easy to see that $\bar{\mathfrak{N}}_1$ is the direct sum of $(\bar{\mathfrak{N}}_1)_{-\beta}$ for $\beta \in L_+$. Therefore it is obvious that the elements η_{ki} of Lemma 45 can be so chosen that η_{ki} is of the rank $-\beta_{ki}$ for some $\beta_{ki} \in L_+$. Now we use the notation of Section 14.

COROLLARY. *Assume that* η_{ki} *is of rank* $-\beta_{ki}$ $(\beta_{ki} \in L_+)$ *in Lemma* 45. *Then*

$$\phi_\lambda(\bar{n}:h;u') = \sum_{1 \leqq i \leqq w} \gamma(q_i:(-1)^{1/2}\lambda)\phi_\lambda(\bar{n}:h;u_i')$$
$$+ \sum_{1 \leqq k \leqq r} \sum_{1 \leqq i \leqq w} e^{-\beta_{ki}(\log h)}\gamma(q_{ki}:(-1)^{1/2}\lambda)\phi_\lambda(\bar{n};\eta_{ki}:h;u_i')$$

for $\lambda \in \mathfrak{F}$, $\bar{n} \in \bar{N}$ *and* $h \in A_{\mathfrak{p}}$.

It follows from Lemma 45 and [2(i), Lemma 18] that

$$\phi_\lambda(x;u') = \sum_i \gamma(q_i:(-1)^{1/2}\lambda)\phi_\lambda(x;u_i') + \sum_{k,i} \gamma(q_{ki}:(-1)^{1/2}\lambda)\phi_\lambda(x;\eta_{ki}u_i')$$

for $x \in G$. Now if we put $x = \bar{n}h$ and observe that

$$\phi_\lambda(\bar{n}h;\eta_{ki}u_i') = e^{-\beta_{ki}(\log h)}\phi_\lambda(\bar{n};\eta_{ki}:h;u_i'),$$

our assertion follows immediately.

Now put

$$\Phi_j(\lambda:\bar{n}:h:H) = \pi_0(\lambda)e^{\rho(\log h+H)}\phi_\lambda(\bar{n}:h\exp H;u_j') \qquad (1 \leqq j \leqq w)$$

for $\lambda \in \mathfrak{F}$, $\bar{n} \in \bar{N}$, $h \in A_{\mathfrak{p}}$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Suppose $Hu_i = \sum_j u_j\gamma(q_{ji})$ where $q_{ji} \in I_{\mathfrak{g}}$. Then we put $\Xi_{ij}(\lambda:H) = \gamma(q_{ji}:(-1)^{1/2}\lambda)$ $(1 \leqq i,j \leqq w)$. It is clear that $\Xi_{ij}(\lambda:H)$ depend on H but not on the particular choice of q_{ji}. Now fix an element $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}^+$. By Lemma 45 we can choose elements q_{ji}, q_{kji} in $I_{\mathfrak{g}}$ and η_{kij} in $\bar{\mathfrak{N}}_1$ $(1 \leqq i,j \leqq w,\ 1 \leqq k \leqq r)$ such that

$$H_0u_i' \equiv \sum_{1 \leqq j \leqq w} u_j'q_{ji} + \sum_{1 \leqq k \leqq r} \sum_{1 \leqq j \leqq w} \eta_{kij}u_j'q_{kji} \bmod \mathfrak{B}\mathfrak{k} \qquad (1 \leqq i \leqq w).$$

Moreover we may assume that η_{kij} is of rank $-\beta_{kij}$ for suitable $\beta_{kij} \in L_+$. Then it follows from the corollary of Lemma 45 that

$$d\Phi_i(\lambda:\bar{n}:h:tH_0)/dt = \sum_{1 \leqq j \leqq w} \gamma(q_{ji}:(-1)^{1/2}\lambda)\Phi_j(\lambda:\bar{n}:h:tH_0)$$
$$+ \sum_{1 \leqq k \leqq r} \sum_{1 \leqq j \leqq w} \gamma(q_{kji}:(-1)^{1/2}\lambda)\Phi_j(\lambda:\bar{n};\eta_{kij}:h:tH_0)$$
$$\times \exp\{-\beta_{kij}(\log h + tH_0)\}.$$

In matrix notation, this equation can be written as follows.

$$d\Phi(\lambda:\bar{n}:h:tH_0)/dt = \Xi(\lambda:H_0)\Phi(\lambda:\bar{n}:h:tH_0) + \Psi(\lambda:\bar{n}:h:t)$$

where

$$\begin{aligned}\Psi_i(\lambda:\bar{n}:h:t) & \\ = \sum_{1\leqq k\leqq r}\ \sum_{1\leqq j\leqq w} & \gamma(q_{kji}:(-1)^{\frac{1}{2}}\lambda)\Phi_j(\lambda:\bar{n};\eta_{kij}:h:tH_0) \\ & \times\exp\{-\beta_{kij}(\log h + tH_0)\}\end{aligned}$$

$(1\leqq i\leqq w)$. Put $\Phi(\lambda:\bar{n}:h:t)=\Phi(\lambda:\bar{n}:h:tH_0), \Phi(\lambda:\bar{n}:h)=\Phi(\lambda:\bar{n}:h:0)$,

$$\begin{aligned}\Phi^0(\lambda:\bar{n}:h:t) &= \exp(-t\Xi(\lambda:H_0))\Phi(\lambda:\bar{n}:h:t), \\ \Psi^0(\lambda:\bar{n}:h:t) &= \exp(-t\Xi(\lambda:H_0))\Psi(\lambda:\bar{n}:h:t) \qquad (t\in R).\end{aligned}$$

Then the following lemma is obvious.

LEMMA 46. *$d\Phi^0(\lambda:\bar{n}:h:t)/dt = \Psi^0(\lambda:\bar{n}:h:t)$ and therefore*

$$\Phi^0(\lambda:\bar{n}:h:T) = \Phi(\lambda:\bar{n}:h) + \int_0^T \Psi^0(\lambda:\bar{n}:h:t)\,dt$$

for $T\geqq 0$.

Put $\beta = \min_{\alpha\in P_+} \alpha(H_0)$ and let ω denote a compact subset of $\mathfrak{F}_R$. It follows from Corollary 2 of Lemma 14 of [2(i)] that $(-1)^{\frac{1}{2}}\lambda(sH_0)$ $(s\in W)$ are all the eigenvalues of $\Xi(\lambda:H_0)$. Hence by Lemma 60 of [2(i)], there exists a positive number c_1 such that $\|\exp(-t\Xi(\lambda:H_0))\|\leqq c_1(1+t)^w$ for $t\geqq 0$ and $\lambda\in\omega$. Put $x^\dagger = \theta(x^{-1})$ as in Section 2 $(x\in G)$. Then $x^\dagger\in KxK$ and therefore $\phi_\lambda(x^\dagger)=\phi_\lambda(x)$. Let $b\rightarrow b^\dagger$ denote the anti-automorphism of $\mathfrak{B}$ such that $X^\dagger = -\theta(X)$ $(X\in\mathfrak{g})$. Then if $\eta\in\bar{\mathfrak{N}}$ and $u\in\mathfrak{H}_{\mathfrak{p}}$, it follows without difficulty that

$$\phi(\lambda:\bar{n};\eta:h;u) = \phi_\lambda(hn;b)$$

where $n=(\bar{n})^\dagger$ and $b=((\eta u)^{\bar{n}})^\dagger$. Therefore since $D(x)\geqq 1$ $(x\in G)$, we get the following result from Theorem 2.

LEMMA 47. *Let U and ω denote two compact subsets of $\bar{N}$ and $\mathfrak{F}_R$ respectively. Then for any $h\in A_{\mathfrak{p}}$, we can select a positive constant c such that*

$$\|\Psi^0(\lambda:\bar{n}:h:t)\|\leqq c(1+t)^w e^{-\beta t}$$

for $\lambda\in\omega$, $\bar{n}\in U$ and $t\geqq 0$.

It is obvious from Lemmas 46 and 47 that $\Phi^0(\lambda:\bar{n}:h:t)$ tends to a limit as $t\rightarrow +\infty$ if $\lambda\in\mathfrak{F}_R$. We denote this limit by $\Phi^0(\lambda:\bar{n}:h:\infty)$.

COROLLARY. *For a fixed h in $A_{\mathfrak{p}}$, $\Phi^0(\lambda:\bar{n}:h:\infty)$ is a continuous function of $(\lambda,\bar{n})$ on $\mathfrak{F}_R\times\bar{N}$.*

It follows from Lemma 47 that the integral $\int_0^\infty \|\Psi^0(\lambda:\bar{n}:h:t)\|\,dt$ converges uniformly as λ and $\bar{n}$ vary in ω and U respectively. The corollary is an immediate consequence of this fact.

As before let $\mathfrak{F}_R'$ be the set of those points λ in $\mathfrak{F}_R$ where $\pi(\lambda)\neq 0$. Fix an open subset ω of $\mathfrak{F}_R'$ such that its closure in $\mathfrak{F}_R'$ is compact. We also assume that $s\omega=\omega$ for $s\in W$. Select an element p in $S(\mathfrak{h}_{\mathfrak{p}})$ and for any $a\in C_c^\infty(\omega)$, put $a_t(\lambda)=a(\lambda)\pi(\lambda)^{-1}p(\lambda)\exp\{-(-1)^{\frac{1}{2}}t\lambda(H_0)\}$ $(t\in R,\lambda\in\mathfrak{F}_R)$. Obviously $a_t\in C_c^\infty(\omega)$ for any t. Now choose an integer $k_0\geqq 0$ such that

$$\int_{\bar{N}} e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}\,d\bar{n}<\infty.$$

LEMMA 48. *Define Ω as in Corollary 1 of Lemma 42 and let b be an element in $\mathfrak{B}$. Then there exists an integer $m\geqq 0$ with the following property. For any $a\in C_c^\infty(\omega)$, we can select a positive number c_a such that*

$$|\phi_{a_t}(\bar{n}h;b)|\leqq c_a(1+t)^m\exp\{-|\rho(\log h)|-\rho(H(\bar{n}))\}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for $\bar{n}\in\bar{N}$, $h\in\Omega$ and $t\geqq 0$.

From Corollary 1 of Lemma 42, we can choose an integer $k_1\geqq 0$ and a positive number c_1 such that

$$|f(\bar{n}h;b)|$$
$$\leqq c_1\exp\{-|\rho(\log h)|-\rho(H(\bar{n}))\}\{1+\rho(H(\bar{n}))\}^{-k_0}\sup_{x\in G}D_{k_1}(x)|f(x;b)|$$

for any $f\in I(G)$. On the other hand by Theorem 3 we can select a finite number of differential operators $d_1,\cdots,d_r$ in $\mathfrak{D}(\mathfrak{h}_{\mathfrak{p}})$ such that

$$\sup_{x\in G}D_{k_1}(x)|\phi_a(x;b)|\leqq\sum_{1\leqq i\leqq r}\sup_{\lambda\in\omega}|a(\lambda;d_i)|$$

for $a\in C_c^\infty(\omega)$. Let m_i denote the order of d_i. Then if $m=\max(m_1,\cdots,m_r)$, it is obvious that for any $a\in C_c^\infty(\omega)$, there exists a positive constant c' such that

$$\sum_{1\leqq i\leqq r}\sup_{\lambda\in\omega}|a_t(\lambda;d_i)|\leqq c'(1+t)^m$$

for all $t\geqq 0$. From this our assertion follows immediately.

COROLLARY 1. *Let u be an element in $\mathfrak{H}_{\mathfrak{p}}$ and η an element in $\bar{\mathfrak{N}}_1$ of rank $-\beta_0$ $(\beta_0\in L_+)$. Then we can select an integer $m\geqq 0$ and, for any $a\in C_c^\infty(\omega)$ and $h\in A_{\mathfrak{p}}$, a positive constant $c(a,h)$ such that*

$$e^{\rho(\log h+tH_0)}\,|\,\phi_{a_t}(\bar{n};\eta:h\exp tH_0;u)\,|\,e^{-\beta_0(\log h+tH_0)}$$
$$\leqq c(a,h)(1+t)^m e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for $\bar{n}\in\bar{N}$ *and* $t\geqq 0$.

This is obvious from the above lemma if we note that

$$\phi_{a_t}(\bar{n};\eta:h\exp tH_0;u)\,e^{-\beta_0(\log h+tH_0)}=\phi_{a_t}(\bar{n}h\exp tH_0;\eta u).$$

For any $a\in C_c^\infty(\omega)$, put

$$\Phi^0(a:\bar{n}:h:t)=\int_{\mathfrak{F}_R}a(\lambda)\Phi^0(\lambda:\bar{n}:h:t)\,d\lambda,$$
$$\Psi^0(a:\bar{n}:h:t)=\int_{\mathfrak{F}_R}a(\lambda)\Psi^0(\lambda:\bar{n}:h:t)\,d\lambda$$

and $\Phi(a:\bar{n}:h)=\Phi^0(a:\bar{n}:h:0)$.

COROLLARY 2. *There exists an integer* $m\geqq 0$ *with the following property. For any* $a\in C_c^\infty(\omega)$ *and* $h\in A_{\mathfrak{p}}$, *we can select a positive number* $c(a,h)$ *such that*

$$\|\Phi^0(a:\bar{n}:h:t)\|\leqq c(a,h)(1+t)^m e^{-\rho(H(\bar{n}))}\{1+\rho(H(\bar{n}))\}^{-k_0}$$

for all $\bar{n}\in\bar{N}$ *and* $t\geqq 0$.

We use the notation of [2(i), Lemma 14]. Put $\lambda^*=(-1)^{\frac{1}{2}}\lambda$ and and $e_{\lambda^*}=\sum_{1\leqq i\leqq w}\sigma^i(\lambda^*)u_i$ $(\lambda\in\mathfrak{F}_R)$. Select $v_{kij}\in J$ such that $u_k u_i=\sum_j v_{kij}u_j$ $(1\leqq k,i\leqq w)$ and put $E_{ij}=\sum_k\sigma^k v_{kij}\in S$. Then it is obvious that

$$e_{\lambda^*}u_i\equiv\sum_{1\leqq j\leqq w}E_{ij}(\lambda^*)u_j \bmod SJ_{\lambda^*} \qquad (1\leqq i\leqq w).$$

Let $E(\lambda^*)$ denote the $w\times w$ matrix with the coefficients $E_{ij}(\lambda^*)$. Then we have seen during the proof of Lemma 51 of [2(i)] that[11]

$$E(s\lambda^*)\Xi(\lambda:H_0)=\Xi(\lambda:H_0)E(s\lambda^*)=s\lambda^*(H_0)E(s\lambda^*) \qquad (s\in W)$$

and $\sum_{s\in W}\epsilon(s)E(s\lambda^*)=\pi(\lambda^*)I$ where I is the unit matrix. Hence

$$\pi(\lambda^*)\exp\{-t\Xi(\lambda:H_0)\}=\sum_{s\in W}\epsilon(s)\exp\{-ts\lambda^*(H_0)\}E(s\lambda^*)$$

for $t\in R$ and $\lambda\in\mathfrak{F}_R$. Therefore

$$\Phi^0(a:\bar{n}:h:t)=\sum_{s\in W}\epsilon(s)\int_{\mathfrak{F}_R}a(\lambda)\pi(\lambda^*)^{-1}$$
$$\times\exp\{-ts\lambda^*(H_0)\}E(s\lambda^*)\Phi(\lambda:\bar{n}:h:t)\,d\lambda.$$

But since $E_{ij}\in S$, the statement of the corollary now follows from Lemma 48.

LEMMA 49. *The integral* $\int_{\bar{N}} \|\Phi^0(a:\bar{n}:h:t)\|\, d\bar{n}$ *is convergent for* $a \in C_c^\infty(\omega)$, $h \in A_{\mathfrak{p}}$ *and* $t \geqq 0$. *Moreover*

$$\int_{\bar{N}} \Phi(a:\bar{n}:h)\, d\bar{n} = \int_{\bar{N}} \Phi^0(a:\bar{n}:h:t)\, d\bar{n} \qquad (t \geqq 0).$$

The first statement is obvious from Corollary 2 of Lemma 48. Moreover it follows from Lemmas 46 and 47 that

$$\Phi^0(a:\bar{n}:h:T) = \Phi(a:\bar{n}:h) + \int_0^T \Psi^0(a:\bar{n}:h:t)\, dt$$

for $T \geqq 0$. On the other hand

$$\Psi^0(a:\bar{n}:h:t) = \sum_{s \in W} \epsilon(s) \int_{\mathfrak{F}_R} a(\lambda)\pi(\lambda^*)^{-1}$$
$$\times \exp\{-ts\lambda^*(H_0)\} E(s\lambda^*)\Psi(\lambda:\bar{n}:h:t)\, d\lambda.$$

Therefore if we take into account the definition of $\Psi(\lambda:\bar{n}:h:t)$, it follows from Corollary 1 of Lemma 48 that

$$\int \| \Psi^0(a:\bar{n}:h:t\|)\, d\bar{n} \leqq c'(1+t)^m \qquad (t \geqq 0),$$

where c' and m are independent of t. This shows that

$$\int_{\bar{N}} d\bar{n} \int_0^T \| \Psi^0(a:\bar{n}:h:t)\|\, dt < \infty.$$

Hence by Fubini's Theorem,

$$\int_{\bar{N}} \Phi^0(a:\bar{n}:h:T)\, d\bar{n} = \int_{\bar{N}} \Phi(a:\bar{n}:h)\, d\bar{n} + \int_0^T dt \int_{\bar{N}} \Psi^0(a:\bar{n}:h:t)\, d\bar{n}.$$

So in order to prove the second statement of the lemma, it is enough to verify that $\int_{\bar{N}} \Psi^0(a:\bar{n}:h:t)\, d\bar{n} = 0$ for any $t \geqq 0$. But in view of the definition of $\Psi(\lambda:\bar{n}:h:t)$ and the expression for $\Psi^0(a:\bar{n}:h:t)$ in terms of $\Psi(\lambda:\bar{n}:h:t)$ given above, it would be sufficient to show that $\int \phi_a(\bar{n};\eta:h;u)\, d\bar{n} = 0$ for $h \in A_{\mathfrak{p}}$, $\eta \in \bar{\mathfrak{N}}_1$, $u \in \mathfrak{H}_{\mathfrak{p}}$ and $a \in C_c^\infty(\omega)$. But this is a consequence of Theorem 3 and Corollary 3 of Lemma 42.

Put $\Phi^0(a:\bar{n}:h:\infty) = \int a(\lambda)\Phi^0(\lambda:\bar{n}:h:\infty)\, d\lambda$ $(a \in C_c^\infty(\omega))$. Then it follows from Lemma 47 that $\Phi^0(a:\bar{n}:h:\infty) = \lim_{t \to +\infty} \Phi(a:\bar{n}:h:t)$. On the other hand

$$\int_{\bar N} \Phi(a:\bar n:h)\,d\bar n = \lim_{t\to+\infty} \int_{\bar N} \Phi^0(a:\bar n:h:t)\,d\bar n$$

by Lemma 49. From these facts we intend to deduce that

$$\int_{\bar N} \Phi_1(a:\bar n:h)\,d\bar n = \int_{\bar N} \Phi_1^0(a:\bar n:h:\infty)\,d\bar n.$$

(Here Φ_1 and Φ_1^0 stand for the first coefficients of the one-column matrices Φ and Φ^0 respectively.) However first let us compute $\Phi_1^0(\lambda:\bar n:h:\infty)$. In order to do this we need the following lemma.

LEMMA 50. *Fix* $\bar n \in \bar N$ *and for* $h \in A_{\mathfrak p}$ *let* h' *denote some element in* $\mathrm{Cl}(A_{\mathfrak p}^+)$ *such that* $\bar n h \in Kh'K$. *Then* $\| \log h' - \log h - H(\bar n) \| \to 0$ *as* $\min_{\alpha\in P_+} \alpha(\log h) \to +\infty$.

Let σ be an irreducible finite-dimensional representation of G on a vector space V and let Λ denote the highest weight of σ. Select an orthonormal base $\psi_0, \psi_1, \cdots, \psi_p$ for V such that ψ_i belongs to the weight Λ_i $0 \leqq i \leqq p$ $(\Lambda_0 = \Lambda)$. Put $\| T \| = (\sum_{0\leqq i\leqq p} | T\psi_i |^2)^{\frac12}$ for any linear transformation T on V. Then

$$\| \sigma(h') \|^2 = \| \sigma(\bar n h) \|^2 = \sum_{0\leqq i\leqq p} | \sigma(\bar n h)\psi_i |^2.$$

Let β_i $(1 \leqq i \leqq p)$ denote the restriction of $\Lambda - \Lambda_i$ on $\mathfrak h_{\mathfrak p}$. Then it follows from [2(e), Lemma 2] that $\beta_i \in L_+$ if $\beta_i \neq 0$. Suppose $\beta_i = 0$ for $1 \leqq i < r$ and $\beta_i \in L_+$ for $r \leqq i \leqq p$. Then the above relation implies that

$$e^{2\Lambda(\log h')} \{ r + \sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')} \}$$
$$= e^{2\Lambda(\log h)} \{ \sum_{0\leqq i< r} | \sigma(\bar n)\psi_i |^2 + \sum_{r\leqq i\leqq p} | \sigma(\bar n)\psi_i |^2 e^{-2\beta_i(\log h)} \}.$$

Now suppose $i < r$ and $\alpha \in P_+$. It is obvious that

$$\sigma(H)\sigma(X_\alpha)\psi_i = \{\Lambda(H) + \alpha(H)\}\sigma(X_\alpha)\psi_i$$

for $H \in \mathfrak h_{\mathfrak p}$. On the other hand α cannot coincide on $\mathfrak h_{\mathfrak p}$ with $-\beta$ for any $\beta \in L_+$. Therefore $\Lambda + \alpha$ cannot coincide on $\mathfrak h_{\mathfrak p}$ with Λ_j for any j $(0 \leqq j \leqq p)$. This implies that $\sigma(X_\alpha)\psi_i = 0$. Hence $\sigma(n)\psi_i = \psi_i$ for $n \in N$ and so $| \sigma(\bar n)\psi_i | = e^{\Lambda(H(\bar n))}$ $(0 \leqq i < r)$. Now put $H'(h) = \log h' - \log h - H(\bar n)$. Then the above equation becomes

$$r + \sum_{r\leqq i\leqq p} | \sigma(\bar n)\psi_i |^2 \exp\{-2\beta_i(\log h) - 2\Lambda(H(\bar n))\}$$
$$= e^{2\Lambda(H'(h))} \{ r + \sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')} \}.$$

Now let $h \to \infty$ in the terminology of Section 9. Then $\beta_i(\log h) \to +\infty$ $(r \leqq i \leqq p)$ and hence we get

$$r = \operatorname*{Lim}_{h\to\infty} e^{2\Lambda(H'(h))} \{r + \sum_{r\leqq i\leqq p} e^{-2\beta_i(\log h')}\} \geqq r \operatorname*{Lim\,sup}_{h\to\infty} e^{2\Lambda(H'(h))}.$$

Since $r \geqq 1$, this shows that $\operatorname*{Lim\,sup}_{h\to\infty} \Lambda(H'(h)) \leqq 0$. On the other hand $\bar{n}h = k_1 h' k_2$ $(k_1, k_2 \in K)$ and therefore $H(\bar{n}) + \log h = H(h'k_2)$. But it follows from Lemma 35 of [2(i)] that $\Lambda(\log h') \geqq \Lambda(H(h'k_2))$ and hence $\Lambda(H'(h)) \geqq 0$. This proves that $\operatorname*{Lim}_{h\to\infty} \Lambda(H'(h)) = 0$. This being true for every highest weight Λ, we conclude from Theorem 1 of [2(a)] that

$$\operatorname*{Lim}_{h\to\infty} \| H'(h) \| = 0.$$

Define the function $\boldsymbol{b}_0$ on $\mathfrak{F}_R$ as in Section 9.

LEMMA 51.[11]

$$\Phi_1{}^0(\lambda : \bar{n} : h : \infty) = e^{-\rho(H(\bar{n}))} \sum_{s\in W} \epsilon_0(s) \boldsymbol{b}_0(s\lambda) \exp\{(-1)^{\frac{1}{2}} s\lambda(\log h + H(\bar{n}))\}$$

for $\lambda \in \mathfrak{F}_R$, $\bar{n} \in \bar{N}$ *and* $h \in A_{\mathfrak{p}}$.

Let $\mathfrak{F}_R''$ be the set of all points $\lambda \in \mathfrak{F}_R$ such that $\lambda(s_1 H_0) \neq \lambda(s_2 H_0)$ for any two distinct elements s_1, s_2 in W. Then $\mathfrak{F}_R'' \subset \mathfrak{F}_R'$ and since $H_0 \in \mathfrak{h}_{\mathfrak{p}_0}{}^+$, it is obvious that $\mathfrak{F}_R''$ is dense in $\mathfrak{F}_R$. Now, for fixed $\bar{n}$ and h, both sides of the above equation are continuous functions of λ (see the corollary of Lemma 47). Therefore it is enough to prove their equality for $\lambda \in \mathfrak{F}_R''$.

Since $\Phi(\lambda : \bar{n} : h : t) = \exp\{t\Xi(\lambda : H_0)\}\Phi^0(\lambda : \bar{n} : h : t)$, it is clear that

$$\pi(\lambda^*)\Phi(\lambda : \bar{n} : h : t) = \sum_{s\in W} \epsilon(s) \exp\{ts\lambda^*(H_0)\} E(s\lambda^*) \Phi^0(\lambda : \bar{n} : h : t)$$

for $t \in R$. (Here the notation is the same as during the proof of Corollary 2 to Lemma 48.) Hence

$$\pi(\lambda^*)\Phi_1(\lambda : \bar{n} : h : t) - \sum_{s\in W} \epsilon(s) \exp\{ts\lambda^*(H_0)\} g_s(\lambda : \bar{n} : h) \to 0$$

as $t \to +\infty$, where

$$g_s(\lambda : \bar{n} : h) = \sum_{1\leqq j\leqq w} E_{1j}(s\lambda^*) \Phi_j{}^0(\lambda : \bar{n} : h : \infty) \qquad (s \in W).$$

On the other hand

$$\Phi_1(\lambda : \bar{n} : h : t) = \pi_0(\lambda) e^{\rho(\log h + tH_0)} \phi_\lambda(\bar{n}h \exp tH_0).$$

Now fix λ, h and $\bar{n}$ $(\lambda \in \mathfrak{F}_R'')$ and for $t \geqq 0$, select an element $h_t' \in \mathrm{Cl}(A_{\mathfrak{p}}{}^+)$ such that $\bar{n}h \exp tH_0 \in Kh_t'K$. Also put $H'(t) = \log h_t' - \log h - tH_0 - H(\bar{n})$.

Then it follows from Lemma 50 that $\| H'(t) \| \to 0$ and therefore $h_t' \to \infty$ (in the termininology of Section 9) as $t \to +\infty$. But

$$e^{\rho(\log h + tH_0)} \phi_\lambda(\bar{n} h \exp tH_0) = \exp\{-\rho(H(\bar{n})) - \rho(H'(t))\} e^{\rho(\log h_t')} \phi_\lambda(h_t')$$

and

$$\lim_{h' \to \infty} | e^{\rho(\log h')} \phi_\lambda(h') - \sum_{s \in W} \boldsymbol{c}(s\lambda) \exp\{s\lambda^*(\log h')\} | = 0$$

from Lemma 37 of [2(i)]. Therefore

$$\Phi_1(\lambda : \bar{n} : h : t) - e^{-\rho(H(\bar{n}))} \sum_{s \in W} \epsilon_0(s) \boldsymbol{b}_0(s\lambda) \exp\{s\lambda^*(\log h + tH_0 + H(\bar{n}))\} \to 0$$

as $t \to +\infty$. This implies that

$$\begin{aligned} &\sum_{s \in W} e^{s\lambda^*(tH_0)} \epsilon(s) g_s(\lambda : \bar{n} : h) \\ &\qquad - e^{-\rho(H(\bar{n}))} \sum_{s \in W} \pi(\lambda^*) \epsilon_0(s) \boldsymbol{b}_0(s\lambda) \exp\{s\lambda^*(\log h + tH_0 + H(\bar{n}))\} \to 0 \end{aligned}$$

as $t \to +\infty$. But since $\lambda \in \mathfrak{F}_R''$, it follows from Lemma 56 of [2(i)] that

$$g_s(\lambda : \bar{n} : h) = \pi(\lambda^*) \epsilon(s) \epsilon_0(s) \boldsymbol{b}_0(s\lambda) e^{-\rho(H(\bar{n}))} \exp\{s\lambda^*(\log h + H(\bar{n}))\} \quad (s \in W).$$

On the other hand $\sum_{s \in W} \epsilon(s) E(s\lambda^*) = \pi(\lambda^*) I$ and therefore

$$\sum_{s \in W} \epsilon(s) g_s(\lambda : \bar{n} : h) = \pi(\lambda^*) \Phi_1{}^0(\lambda : \bar{n} : h : \infty).$$

Hence

$$\begin{aligned} &\pi(\lambda^*) \Phi_1{}^0(\lambda : \bar{n} : h : \infty) \\ &\qquad = \pi(\lambda^*) e^{-\rho(H(\bar{n}))} \sum_{s \in W} \epsilon_0(s) \boldsymbol{b}_0(s\lambda) \exp\{s\lambda^*(\log h + H(\bar{n}))\}. \end{aligned}$$

The statement of the lemma is now obvious since $\pi(\lambda^*) \neq 0$.

COROLLARY. *The integral* $\int_{\bar{N}} | \Phi_1{}^0(a : \bar{n} : h : \infty) | \, d\bar{n}$ *converges if* $a \in C_c{}^\infty(\omega)$ *and* $h \in A_{\mathfrak{p}}$.

Fix h and a. Then it is obvious that for any $s \in W$,

$$\sup_{H \in \mathfrak{h}_{\mathfrak{p}_0}} (1 + \| H \|)^{k_0} | \int_{\mathfrak{F}_R} \boldsymbol{b}_0(s\lambda) a(\lambda) \exp\{s\lambda^*(\log h + H)\} d\lambda | < \infty.$$

Hence there exists a positive number c such that

$$| \Phi_1{}^0(a : \bar{n} : h : \infty) | \leqq c(1 + \| H(\bar{n}) \|)^{-k_0} e^{-\rho(H(\bar{n}))} \qquad (\bar{n} \in \bar{N})$$

and from this the corollary follows immediately.

Now we regard the Lie group $\bar{N}$ as an analytic manifold. For any $\nu \in C_c^\infty(\bar{N})$ and $a \in C_c^\infty(\omega)$, put

$$\Phi^0(a:\nu:\bar{n}_0:h:t) = \int_{\bar{N}} \nu(\bar{n})\Phi^0(a:\bar{n}_0\bar{n}:h:t)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}, h \in A_{\mathfrak{p}}, t \geqq 0)$$

and $\Phi(a:\nu:\bar{n}_0:h) = \Phi^0(a:\nu:\bar{n}_0:h:0)$. It follows from the corollary of Lemma 47 that the integral

$$\Phi^0(a:\nu:\bar{n}_0:h:\infty) = \int_{\bar{N}} \nu(\bar{n})\Phi^0(a:\bar{n}_0\bar{n}:h:\infty)\,d\bar{n}$$

is also well defined.

LEMMA 52. *The integrals*

$$\int_{\bar{N}} \Phi(a:\nu:\bar{n}:h)\,d\bar{n}, \qquad \int_{\bar{N}} \Phi^0(a:\nu:\bar{n}:h:\infty)\,d\bar{n}$$

are both well defined for $a \in C_c^\infty(\omega)$, $\nu \in C_c^\infty(\bar{N})$, $h \in A_{\mathfrak{p}}$ *and they are equal.*

In view of Lemma 49 and the right-invariance of the Haar measure of the nilpotent group $\bar{N}$, it is clear that

$$\int \|\Phi(a:\nu:\bar{n}:h)\|\,d\bar{n} \leqq \int |\nu(\bar{n})|\,d\bar{n} \int \|\Phi(a:\bar{n}:h)\|\,d\bar{n} < \infty.$$

Moreover it follows from Lemmas 46 and 47 that

$$\Phi^0(a:\nu:\bar{n}:h:\infty) = \Phi(a:\nu:\bar{n}:h) + \int_0^\infty \Psi^0(a:\nu:\bar{n}:h:t)\,dt$$

where

$$\Psi^0(a:\nu:\bar{n}_0:h:t) = \int \nu(\bar{n})\Psi^0(a:\bar{n}_0\bar{n}:h:t)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}).$$

We claim that

$$\int_{\bar{N}} d\bar{n} \int_0^\infty \|\Psi^0(a:\nu:\bar{n}:h:t)\|\,dt < \infty.$$

If we recall the definition of $\Psi^0(\lambda:\bar{n}:h:t)$ $(\lambda \in \mathfrak{F}_R)$, it becomes clear (see the proof of Lemma 49) that for this it would be sufficient to prove the following lemma. Put $\phi_a(\bar{n}:h) = \phi_a(\bar{n}h)$ $(a \in C_c^\infty(\omega))$ and use the notation of Corollary 1 of Lemma 48.

LEMMA 53. *For any* $a \in C_c^\infty(\omega)$ *and* $\nu \in C_c^\infty(\bar{N})$, *put*

$$\phi_a(\nu:\bar{n}_0:h) = \int_{\bar{N}} \nu(\bar{n})\phi_a(\bar{n}_0\bar{n}:h)\,d\bar{n} \qquad (\bar{n}_0 \in \bar{N}, h \in A_{\mathfrak{p}}).$$

Then for any $u \in \mathfrak{H}_{\mathfrak{p}}$ *and* $h \in A_{\mathfrak{p}}$, *the integral*

$$\int_{\bar N} d\bar n \int_0^\infty | \phi_{a_t}(\nu : \bar n ; \eta : h \exp tH_0 ; u) | \times \exp\{\rho(\log h + tH_0) - \beta_0(\log h + tH_0)\} dt$$

is finite.

Let $\xi \to \xi'$ denote the anti-automorphism of $\bar{\mathfrak{N}}$ such that $X' = -X$ $(X \in \bar{\mathfrak{n}})$. Then in view of the left-invariance of the measure $d\bar n$, it is clear that

$$\phi_a(\nu : \bar n ; \eta : h ; u) = \phi_a(\nu' : \bar n : h ; u),$$

where $\nu'(\bar n^{-1}) = \nu(\bar n^{-1} ; (\eta')^{\bar n})$ $(\bar n \in \bar N)$. Hence $\phi_{a_t}(\nu : \bar n ; \eta : h \exp tH_0 ; u) = \phi_{a_t}(\nu' : \bar n : h \exp tH_0 ; u)$. Now fix ν, h and a. Then from Lemma 48, we can choose a positive constant c and an integer $m \geqq 0$ such that

$$| \phi_{a_t}(\nu' : \bar n_0 : h \exp tH_0 ; u) | e^{\rho(\log h + tH_0)} \leqq c(1+t)^m \int | \nu'(\bar n) | e^{-\rho(H(\bar n_0 \bar n))} \{1 + \rho(H(\bar n_0 \bar n))\}^{-k_0} d\bar n$$

for all $\bar n_0 \in \bar N$ and $t \geqq 0$. Since $\beta_0(H_0) > 0$, the assertion of the lemma is now obvious.

This proves that

$$\int \| \Phi^0(a : \nu : \bar n : h : \infty) \| d\bar n \leqq \int \| \Phi(a : \nu : \bar n : h) \| d\bar n + \int d\bar n \int_0^\infty \| \Psi^0(a : \nu : \bar n : h : t) \| dt < \infty .$$

Therefore it follows by Fubini's Theorem that

$$\int \Phi^0(a : \nu : \bar n : h : \infty) d\bar n = \int \Phi(a : \nu : \bar n : h) d\bar n + \int_0^\infty dt \int \Psi^0(a : \nu : \bar n : h : t) d\bar n .$$

Hence in order to prove Lemma 52, it would be sufficient to verify that

$$\int \Psi^0(a : \nu : \bar n : h : t) d\bar n = 0$$

for any $t \geqq 0$. But we have seen during the proof of Lemma 49 that the integral $\int | \Psi^0(a : \bar n : h : t) \| d\bar n$ is finite and $\int \Psi^0(a : \bar n : h : t) d\bar n = 0$. Hence it is obvious that

$$\int \Psi^0(a : \nu : \bar n : h : t) d\bar n = \int \nu(\bar n) d\bar n \int \Psi^0(a : \bar n : h : t) d\bar n = 0.$$

This completes the proof of Lemma 52.

Now select ν in such a way that $\int \nu(\bar{n})\,d\bar{n} = 1$. Then it follows from Lemmas 52 and 49 and the corollary of Lemma 51 that

$$\int \Phi_1{}^0(a:\bar{n}:h:\infty)\,d\bar{n} = \int \Phi_1{}^0(a:\nu:\bar{n}:h:\infty)\,d\bar{n}$$
$$= \int \Phi_1(a:\nu:\bar{n}:h)\,d\bar{n} = \int \Phi_1(a:\bar{n}:h)\,d\bar{n}$$

for $a \in C_c{}^\infty(\omega)$ and $h \in A_{\mathfrak{p}}$. Now fix a and h and put

$$a_s'(H) = \int \boldsymbol{b}_0(s\lambda)a(\lambda)\exp\{s\lambda^*(\log h + H)\}\,d\lambda$$

for $s \in W$ and $H \in \mathfrak{h}_{\mathfrak{p}_0}$. Then it follows from the theory of Fourier transforms that $\sup\limits_{H \in \mathfrak{h}_{\mathfrak{p}_0}} (1 + \| H \|)^{k_0} | a_s'(H) | < \infty$. On the other hand,

$$\Phi_1{}^0(a:\bar{n}:h:\infty) = e^{-\rho(H(\bar{n}))} \sum_{s \in W} \epsilon_0(s) a_s'(H(\bar{n}))$$

by Lemma 51. Therefore it is obvious that

$$\int \Phi_1{}^0(a:\bar{n}:h:\infty)\,d\bar{n} = \sum_{s \in W} \epsilon_0(s) \int a_s'(H(\bar{n}))\,e^{-\rho(H(\bar{n}))}\,d\bar{n}.$$

Now let δ be a sufficiently small positive number. By the corollary of Lemma 45 of [2(i)], $\int \exp\{-(1+\delta)\rho(H(\bar{n}))\}\,d\bar{n} < \infty$ and therefore, by Fubini's Theorem,

$$\int a_s'(H(\bar{n}))\exp\{-(1+\delta)\rho(H(\bar{n}))\}\,d\bar{n}$$
$$= \int \boldsymbol{b}_0(s\lambda)a(\lambda)e^{s\lambda^*(\log h)}\,d\lambda \int \exp\{s\lambda^*(H(\bar{n})) - (1+\delta)\rho(H(\bar{n}))\}\,d\bar{n}$$
$$= \int \boldsymbol{b}_0(\lambda)a(s^{-1}\lambda)\mathrm{e}^{\lambda^*(\log h)}\operatorname{conj}\boldsymbol{c}(\lambda_\delta)\,d\lambda$$

from Theorem 4 of [2(i)], where $\lambda_\delta = \lambda - (-1)^{\frac{1}{2}}\delta\rho$. But since $\omega \subset \mathfrak{F}_R'$, $\boldsymbol{c}$ is a holomorphic function on a complex neighborhood of ω in $\mathfrak{F}$. Therefore if we recall that ω is invariant under W, it becomes obvious that

$$\int a_s'(H(\bar{n}))\,e^{-\rho(H(\bar{n}))}\,d\bar{n} = \lim_{\delta \to 0} \int a_s'(H(\bar{n}))\,e^{-(1+\delta)\rho(H(\bar{n}))}\,d\bar{n}$$
$$= \int \boldsymbol{b}_0(\lambda)a(s^{-1}\lambda)\,e^{\lambda^*(\log h)}\operatorname{conj}\boldsymbol{c}(\lambda)\,d\lambda$$
$$= \int | \boldsymbol{b}_0(\lambda) |^2 \pi_0(\lambda)^{-1} a(s^{-1}\lambda)\,e^{\lambda^*(\log h)}\,d\lambda.$$

Hence

$$\int \Phi_1^0(a:\bar{n}:h:\infty)\,d\bar{n} = \int \mid \boldsymbol{b}_0(\lambda)\mid^2 \{\pi_0(\lambda)^{-1} \sum_{s\in W} \epsilon_0(s)a(s\lambda)\}e^{\lambda^*(\log h)}d\lambda.$$

But we have seen above that

$$\int \Phi_1^0(a:\bar{n}:h:\infty)\,d\bar{n} = \int \Phi_1(a:\bar{n}:h)\,d\bar{n} = e^{\rho(\log h)} \int \phi_a(\bar{n}h)\,d\bar{n}.$$

Therefore it follows easily from the corollary of Lemma 43 that $\boldsymbol{\beta}(\lambda) = \mid \boldsymbol{b}_0(\lambda)\mid^2$ for $\lambda \in \omega$. But since this holds for any choice of ω and since $\boldsymbol{\beta}$ and $\boldsymbol{b}_0$ are both continuous on $\mathfrak{F}_R$, it is obvious that this relation actually holds for all $\lambda \in \mathfrak{F}_R$.

THEOREM 4. *Let a be an element in $\mathcal{C}(\mathfrak{F}_R)$. Then*

$$e^{\rho(H)} \int_{\bar{N}} \phi_a(\bar{n}\exp H)\,d\bar{n} = \int_{\mathfrak{F}_R} \mid \boldsymbol{b}_0(\lambda)\mid^2 \{\pi_0(\lambda)^{-1} \sum_{s\in W} \epsilon_0(s)a(s\lambda)\}e^{(-1)^{\frac{1}{2}}\lambda(H)}d\lambda$$

for $H \in \mathfrak{h}_{\mathfrak{p}_0}$.

In view of the result obtained above, this is an immediate consequence of the corollary of Lemma 43, if we use the regular normalization of $d\lambda$. On the other hand the statement of the theorem is obviously independent of the normalization of $d\lambda$. Hence it holds in general.

THEOREM 5. *Let $a \in \mathcal{C}(\mathfrak{F}_R)$ and $\lambda \in \mathfrak{F}_R$. Then*

$$\pi_0(\lambda) \int_G \phi_a(x)\operatorname{conj}\phi_\lambda(x)\,dx = \mid \boldsymbol{b}_0(\lambda)\mid^2 \sum_{s\in W} \epsilon_0(s)a(s\lambda)$$

if we use the regular normalizations of dx and $d\lambda$.

This is merely a restatement of the corollary of Lemma 41.

COROLLARY 1. *Let w denote the order of W. Then under the above normalizations,*

$$\int_G \mid \phi_a(x)\mid^2 dx = w^{-1} \int_{\mathfrak{F}_R} \mid \boldsymbol{b}_0(\lambda)\mid^2 \mid \sum_{s\in W} \epsilon_0(s)a(s\lambda)\mid^2 d\lambda$$

for $a \in \mathcal{C}(\mathfrak{F}_R)$.

This would follow immediately from Theorem 5 by Fubini's Theorem, as soon as we can verify that

$$\int |\pi_0(\lambda)a(\lambda)\phi_\lambda(x)\phi_a(x)|\,dxd\lambda < \infty.$$

This is done as follows. We know (see [2(f), § 12]) that if the Haar measure dh on $A_{\mathfrak{p}}$ is suitably normalized,

$$\int f(x)\,dx = \int_{A_{\mathfrak{p}}^+} f(h)\Delta(h)\,dh$$

for any spherical function f in $C_c(G)$. (Here Δ has the same meaning as in Section 13.) Now select an integer $q \geqq 0$ such that

$$c_1 = \int_{A_{\mathfrak{p}}} (1 + \|\log h\|)^{-q}\,dh < \infty.$$

Then

$$|\pi_0(\lambda)| \int |\phi_\lambda(x)\phi_a(x)|\,dx = |\pi_0(\lambda)| \int_{A_{\mathfrak{p}}^+} |\phi_\lambda(h)\phi_a(h)|\,\Delta(h)\,dh$$
$$\leqq c_1 \sup_{h \in A_{\mathfrak{p}}^+} \Delta(h)(1 + \|\log h\|)^q\,|\pi_0(\lambda)\phi_\lambda(h)\phi_a(h)|.$$

Hence it follows from Theorems 1 and 3 that there exists an integer $k \geqq 0$ and, for a fixed a, a positive number c such that

$$|\pi_0(\lambda)| \int |\phi_\lambda(x)\phi_a(x)|\,dx \leqq c(1 + \|\lambda\|)^k$$

for all $\lambda \in \mathfrak{F}_R$. Therefore

$$\int |\pi_0(\lambda)a(\lambda)\phi_\lambda(x)\phi_a(x)|\,dxd\lambda \leqq c\int (1 + \|\lambda\|)^k\,|a(\lambda)|\,d\lambda < \infty.$$

Let $I_0(G)$ denote the subspace of $I(G)$ consisting of all elements of the form ϕ_a $(a \in \mathcal{C}(\mathfrak{F}_R))$.

COROLLARY 2. *For any f in $I(G)$, put*

$$\bar{f}(\lambda) = \int_G f(x)\,\mathrm{conj}\,\phi_\lambda(x)\,dx \qquad (\lambda \in \mathfrak{F}_R).$$

Then

$$\int_G |f(x)|^2\,dx = w^{-1}\int_{\mathfrak{F}_R} |\boldsymbol{c}(\lambda)|^{-2}\,|\bar{f}(\lambda)|^2\,d\lambda$$

and

$$f(x) = w^{-1} \int_{\mathfrak{F}_R} |\boldsymbol{c}(\lambda)|^{-2} \bar{f}(\lambda) \phi_\lambda(x)\, d\lambda$$

for $f \in I_0(G)$ *and* $x \in G$, *if* dx *and* $d\lambda$ *are regularly normalized.*

This is an immediate consequence of Theorems 5 and Corollary 1 above. We have seen (Lemma 29) that $\boldsymbol{c}^{-1}$ is analytic on $\mathfrak{F}_R$. Moreover Theorem 5 of [2(i)] gives a geometric interpretation of $\boldsymbol{c}$.

16. Two conjectures. Let $I_c(G)$ denote the subspace consisting of those elements of $I(G)$ which have compact support. Also let $L_2(G)$ denote the Hilbert space of square-integrable functions on G and $I_2(G)$ the closure of $I_c(G)$ in $L_2(G)$. It is seen without difficulty that $I_c(G) \subset I(G) \subset I_2(G)$. Therefore if the statements of Corollary 2 of Theorem 5 could be extended to all functions $f \in I(G)$, we would immediately get an explicit Plancherel formula (see [2(j)]) for $I_2(G)$. Moreover Theorem 5 of [2(i)] would then provide a simple interpretation for the Plancherel measure. For this, it would obviously be enough to show that $I_c(G) \subset I_0(G)$. However this appears to be a rather difficult problem which I have not yet been able to solve. Its solution seems to depend on the following two unproved statements.

(1) *There exists a polynomial function* $p \in S(\mathfrak{h}_\mathfrak{p})$ *such that* $|\boldsymbol{b}_0(\lambda)p(\lambda)| \geqq 1$ *for all* $\lambda \in \mathfrak{F}_R$.

(2) *For any* $f \in I(G)$, *define* F_f *as in Corollary* 4 *to Lemma* 42. *Then* $F_f \neq 0$ *unless* $f = 0$.

Assuming these two conjectures, we shall show that $I_c(G) \subset I_0(G)$. Let f be any element in $I_c(G)$. Then it follows from Lemma 43 and Corollary 4 of Lemma 42 that $\bar{f} \in \mathscr{B}(\mathfrak{F}_R)$. On the other hand if we take Lemma 31 into account, it follows from the first conjecture that the function $a(\lambda) = w^{-1}\pi_0(\lambda)|\boldsymbol{b}_0(\lambda)|^{-2}\bar{f}(\lambda)$ $(\lambda \in \mathfrak{F}_R)$ also lies in $\mathscr{B}(\mathfrak{F}_R)$. Now put $g = \phi_a$. We know from the corollary of Lemma 17 of [2(i)] that $\phi_{s\lambda} = \phi_\lambda (s \in W)$ and therefore $\bar{f}(s\lambda) = \bar{f}(\lambda)$ and $\pi_0(\lambda)\bar{g}(\lambda) = \pi_0(\lambda)\bar{f}(\lambda)$ $(\lambda \in \mathfrak{F}_R)$ by Theorem 5. Moreover $\bar{g}$ and $\bar{f}$ are both continuous functions on $\mathfrak{F}_R$ (see Corollary 3 of Lemma 40). Hence $\bar{g} = \bar{f}$. But then by Lemma 43, $F_f = F_g$ and therefore $f = g = \phi_a$ by the second conjecture. This proves that $f \in I_0(G)$ and therefore $I_c(G) \subset I_0(G)$.

Although there seems to be considerable evidence in support of these conjectures, I have at present no clear idea as to how to proceed to prove them.

COLUMBIA UNIVERSITY.

REFERENCES.

[1] L. Garding, *Math. Scand.*, vol. 1 (1953), pp. 55-72.

[2] Harish-Chandra, (a) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
(b) " " " " vol. 75 (1953), pp. 185-243.
(c) " " " " vol. 76 (1954), pp. 234-253.
(d) " " " " vol. 83 (1956), pp. 98-163.
(e) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(f) " " " vol. 78 (1956), pp. 564-628.
(g) " " " vol. 79 (1957), pp. 87-120.
(h) " " " vol. 79 (1957), pp. 193-257.
(i) " " " vol. 80 (1958), pp. 241-310.
(j) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 40 (1954), pp. 200-204.
(k) " " " " " vol. 43 (1957), pp. 408-409.

[3] F. John, *Proceedings of the Symposium on Spectral Theory and Differential Problems*, Stillwater, Okla., 1951, pp. 113-175.

[4] L. Schwartz, *Théorie des distributions I*, Paris, Hermann, 1950.

ON NILALGEBRAS AND LINEAR VARIETIES OF NILPOTENT MATRICES, I.*

By MURRAY GERSTENHABER.[1]

Let $A_1, \cdots, A_k$ be $n \times n$ matrices with coefficients in a field K having at least n elements, and which have the property that every linear combination of them with coefficients in K is nilpotent. The main purpose of this paper is then to demonstrate that $k \leqq n(n-1)/2$ and if in fact $k = n(n-1)/2$, that there exists a matrix C with coefficients in K such that the CA_iC^{-1} are all triangular matrices. Letting V denote the subspace of n^2-space of all linear combinations of $A_1, \cdots, A_k$, one may say: $\dim V \leqq n(n-1)/2$ and if $\dim V = n(n-1)/2$, then V is in fact an algebra, and one may choose a new basis for the space on which V operates relative to which V is just the algebra of all triangular matrices, where here a triangular matrix shall be one with zeros both below and on the diagonal. For the matrix C of the change of basis one can choose any matrix transforming an arbitrary element of V with nilindex exactly n into triangular form; from what has been asserted, it follows that V indeed contains such an element of maximal nilindex.

The assumption that K has at least n elements is used, as will be seen, to insure that if K' is any extension of K and $V_{K'}$ the linear space obtained by extending the field of definition of V to K', then it is still the case that that every matrix in $V_{K'}$ is nilpotent; one may then say of the variety determined by V that every element in it is nilpotent.

It is easy to exhibit a pair of $n \times n$ matrices with coefficients in a field of fewer than n elements all of whose linear combinations over that field are nilpotent but not over a larger one. Nevertheless, S. A. Hoffman has shown [unpublished] that if three 3×3 matrices with coefficients in the field of two elements have the property that all their linear combinations over that field are nilpotent, then it is still the case that they can simultaneously be brought to triangular form. This suggests that the assumption that K have at least n elements may be unnecessary; no counterexample is yet known to the author.

---

* Received October 11, 1957; revised January 23, 1958.

[1] The author gratefully wishes to acknowledge the support of the National Science Foundation through contract NSF G-2270 with the University of Pennsylvania.

Proof of the theorem. A necessary and sufficient condition that an $n \times n$ matrix M be nilpotent is that the sum $s_r(M)$ of its $r \times r$ principal minors vanish for all $r = 1, \cdots, n$, for these sums are, up to sign, the coefficients of the characteristic polynomial of M. Let V denote always the given vector space of nilpotent matrices defined over a coefficient field K. If A, B are in V, then $\alpha A + B$ is in V for every α in K, hence is nilpotent, and $s_r(\alpha A + B) = 0$ for $r = 1, \cdots, n$. The expression $s_r(\alpha A + B)$ may be written as a polynomial in α of degree $r - 1$, say

$$s_r(\alpha A + B) = \alpha^{r-1} s_{r,r-1} + \alpha^{r-2} s_{r,r-2} + \cdots + \alpha s_{r,1}, \text{ where } s_{r,i}$$

is simultaneously a homogeneous form of degree i in the coefficients of A and of degree $r - i$ in the coefficients of B. Keeping r fixed and letting α range through the non-zero elements of K, the equations $s_r(\alpha A + B) = 0$ may be viewed as a system of homogeneous linear equations for the $r - 1$ unknowns $s_{r,i}$. Since $r \leqq n$, there are, by assumption, at least $r - 1$ distinct non-zero elements of K. Choosing such a set of elements, the determinant of the system is of Vandermonde type and does not vanish; therefore $s_{r,i} = 0$ for all r and i. It follows that $s_r(xA + B) = 0$ for x in any extension K' of K, whence $xA + B$ is nilpotent. Equivalently, $x_1 A_1 + x_2 A_2$ is nilpotent, where x_1, x_2 are arbitrary elements of K' and A_1, A_2 are arbitrary elements of V. Now if it has been shown that any linear combination of, say, t elements of V with coefficients in K' is nilpotent, then it follows that

$$x_1 A_1 + \cdots + x_{t-1} A_{t-1} + x_t (A_t + \alpha A_{t+1})$$

is nilpotent for all $x_1, \cdots, x_t$ in K', $A_1, \cdots, A_{t+1}$ in V, and α in K. By the same argument as that just given, it follows that one may again replace α by an element of K', whence $x_1 A_1 + \cdots + x_t A_t + x_{t+1} A_{t+1}$ is also nilpotent for all $x_1, \cdots, x_{t+1}$ in K', and by induction, this holds for all t. We may, therefore, whenever it is suitable, enlarge the field of definition for V, and it will remain the case that every matrix in the enlarged linear space is nilpotent. Therefore, in general, no subscript will be used to indicate the field of definition, particularly when it is clear from the context.

If the linear variety V is spanned by $A_1, \cdots, A_k$, then a generic element of V over K is a matrix of the form $x_1 A_1 + \cdots + x_k A_k$, where $(x) = (x_1, \cdots, x_k)$ is a set of k independent transcendentals over K. The elements of this generic matrix are linear functions l_{ij} of $x_1, \cdots, x_k$ and may be viewed as vectors in a k-dimensional space with components $((A_1)_{ij}, \cdots, (A_k)_{ij})$. This set of vectors indexed by pairs of indices (i, j), $i, j = 1, \cdots, n$ may be considered associated with the variety V and uniquely determines it. For convenience, we shall occasionally denote a pair of indices (i,j) by a single symbol, say σ, and the corresponding vector by l_σ. Among the vectors l_σ the number of linearly independent ones is $\dim V$.

If X is any $n \times n$ matrix with coefficients in an extension field of K and with non-vanishing determinant, then we may form the linear variety $V(X) = XVX^{-1}$ defined over the field $K(X) = K((x_{ij}))$; it has the same dimension as V, and every matrix in it is again nilpotent. The vectors associated with $V(X)$ will be denoted by $l_{ij}(X)$ or $l_\sigma(X)$; for $X = 1$, we will write as before just l_σ. If S is a subset of the set of all pairs of indices (i,j), $i,j = 1, \cdots, n$, then the linear space spanned by the $l_\sigma(X)$, $\sigma \in S$, will be denoted by $L_S(X)$. If S and S' are two sets of pairs of indices such that $L_{S'}(X) \subseteq L_S(X)$, then S' will be said to be dependent on S; such dependencies usually vary with X. Further, if $\dim L_S(X) = \dim V$, then every S' is dependent on S and S will be called complete.

Given τ, S, and X such that $l_\tau(X) \in L_S(X)$, then we may write $l_\tau(X) = \sum a_\sigma(X) l_\sigma(X)$, the summation ranging over $\sigma \in S$, where $a_\sigma(X)$ is an element of $K(X)$. If Y is a specialization of X over K with non-zero determinant, it does not necessarily follow that $l_\tau(Y) \in L_S(Y)$; for some $a_\sigma(Y)$ may not be finite, although, since there always exists a σ_0 for which all $a_\sigma(Y)/a_{\sigma_0}(Y)$ are finite [1], one finds, in that case, a dependence relation between the $l_\sigma(Y)$ for $\sigma \in S$. However, if Y is a generic specialization of X, then certainly all $a_\sigma(Y)$ are finite and we may write $l_\tau(Y) = \sum a_\sigma(Y) l_\sigma(Y)$.

The set of all pairs of indices (i,j), $i,j = 1, \cdots, n$, may be divided naturally into three disjoint subsets: δ_+, the set of all (i,j) with $j > i$, i.e., the elements above the diagonial; δ_0, the set of all (i,j) on the diagonal; and δ_-,the set of all (i,j) with $j < i$, or the elements below the diagonal. Given a $\sigma = (i,j)$, we may occsionally write σ^* for the pair (j,i). The set of all σ^* for σ in a set S will then be denoted by S^*. Instead of L_{δ_+}, we will write simply L_+; analogous definitions will hold for L_0 and L_-.

For a linear variety of nilpotent matrices, it is always the case that δ_0 is dependent on δ_+ (and, of course, δ_-), else there would exist a matrix in V with zero entries above the diagnoal and a non-zero entry somewhere on the diagonal; but such a matrix can not be nilpotent. Since $V(X) = XVX^{-1}$ is also a linear variety of nilpotent matrices, the same holds for it. From this will follow now the first major lemma in the proof of our proposition: Let X be a matrix whose elements are n^2 independent transcendental quantities over K, the field of definition for V. Then $L_+(X)$ is complete.

Since $L_0(X) \subseteq L_+(X)$, were this false there would exist a $\tau = (i,j)$

in δ_- such that $l_\tau(X) \notin L_+(X)$; assume τ so chosen that $i - j$ is minimal. To see that this leads to a contradiction, we shall consider the effect of replacing X by $X' = (1 + z e_{\tau^*})X$, where z is transcendental over $K(X)$ and e_{τ^*} is the matrix with 1 in the j-th row, i-th column, and zeros elsewhere. Given a matrix A, the matrix $(1 + z e_{\tau^*}) A (1 + z e_{\tau^*})^{-1}$ is obtained from A by adding z times the i-th row to the j-th and then subtracting z times the j-th column from the i-th (for note that $(1 + z e_{\tau^*})^{-1} = 1 - z e_{\tau^*}$). Let now S denote $\delta_+ - \tau^*$. Then it is the case that $L_S(X') \subseteq L_S(X)$. For if $\sigma \in \delta_+$ but σ not in the j-th row or i-th column, then $l_\sigma(X') = l_\sigma(X)$. If $\sigma \in \delta_+$ and σ in the j-th row but $\sigma \neq \tau^*$, then we may set $\sigma = (j, k)$ and $l_{jk}(X') = l_{jk}(X) + z l_{ik}(X)$. Here $k > j$, and by choice of τ, for such k, we have $l_{ik}(X) \in L_+(X)$ (for note that this is so for $k > j$ but $k < i$ by choice of τ; that $l_{ii}(X) \in L_+(X)$ since δ_0 is dependent on δ_+; and that $l_{ik}(X) \in L_+(X)$ by definition for $k > i$). Therefore, $l_{jk}(X')$, being a linear combination of elements of $L_+(X)$, is in $L_+(X)$, where, however, we must now construe $L_+(X)$ as a vector space over $K(X, z)$. Similarly, for $\sigma \in \delta_+$, σ in the i-th column but $\sigma \neq \tau^*$, we have $\sigma = (k, i)$ and $l_{ki}(X') = l_{ki}(X) - z l_{kj}(X)$. Therefore, for all $\sigma \in S$, we have $l_\sigma(X') \in L_S(X)$, so $L_S(X') \subseteq L_S(X)$. However, for $l_{\tau^*}(X')$, we have $l_{\tau^*}(X') = l_{\tau^*}(X) + z l_{ii}(X) - z l_{jj}(X) - z^2 l_\tau(X)$, and for $l_{jj}(X')$, we have $l_{jj}(X') = l_{jj}(X) + x l_\tau(X)$. Now $l_{jj}(X')$ is in $L_+(X')$, and from these equations and the fact that $l_{\tau^*}(X)$ and $l_{jj}(X)$ are in $L_+(X)$ but $l_\tau(X)$ is not, it follows that $l_{jj}(X') = -z^{-1} l_{\tau^*}(X') + \sum a_\sigma(X') l_\sigma(X')$, where the sumation ranges over σ in S. Therefore,

$$z l_{jj}(X') = - l_{\tau^*}(X') + z \sum a_\sigma(X') l_\sigma(X'),$$

and this is an identity in z, where X' may be considered a function of z taking on the value X when $z = 0$. Since the entries in X are independent transcendentals over K, it is the case that any matrix X' is a specialization of X over K, but since z is transcendental over $K(X)$, it follows that the entries in X' are likewise independent transcendentals over K; so X and X' are generic specializations of each other. Therefore $a_\sigma(X)$ is finite for all $\sigma \in S$, and setting $z = 0$, we find $l_{\tau^*}(X) = 0$. But again, since X' is a generic specialization of X, it follows that $l_{\tau^*}(X') = 0$, and from the equation for $l_{\tau^*}(X')$, we find $0 = z l_{ii}(X) - z l_{jj}(X) - z^2 l_\tau(X)$ which implies that $l_\tau(X) \in L_0(X) \subseteq L_+(X)$, contrary to assumption. Therefore, indeed, if the elements of X are n^2 independent transcendental quantities over K, then $L_+(X)$ is complete.

Since δ_+ contains only $n(n-1)/2$ elements, it follows that $\dim V \leq n(n-1)/2$, which proves the first half of our main proposition. We shall suppose henceforth that $\dim V = n(n-1)/2$, and we must show that V is then similar to the set of all triangular matrices. Since by choosing X a generic $n \times n$ matrix over the field K of definition for V, we have $L_+(X)$ complete, we shall henceforth assume simply that the transformation has been made and L_+ is complete. We must assume, however, that the field of definition, K, has been extended to $K(X)$, a pure transcendental extension of dimension n^2 over K.

Let P now be any invertible $n \times n$ matrix with zeroes above the diagonal and remaining coefficients in $K(X)$. We may form $V(P) = PVP^{-1}$ and $L_+(P)$. It is then the case that $L_+(P) = L_+$. For if A is any matrix in V and P, as before, has zeros above the diagonal, then the i-th row of PA is a linear combination only of rows $1, \cdots, i$ of A. Similarly, if Q has zeros above the diagonal, then the j-th column of AQ is a linear combination of columns $1, \cdots, j$, and P^{-1} is such a Q. Therefore, if $\sigma \in \delta_+$, then $l_\sigma(P)$ is a linear combination of l_σ's for $\sigma \in \delta_+$, so $L_+(P) \subseteq L_+$. Transforming by P^{-1}, the reverse inclusion holds, so indeed $L_+(P) = L_+$.

Suppose now that $\dim V = n(n-1)/2$ and that L_+ be complete. Since δ_+ has only $n(n-1)/2$ elements, there must exist a matrix $A = (a_{ij})$ in V for which $a_{i,i+1} = 1$, $i = 1, \cdots, n-1$, and $a_{ij} = 0$ for $j > i+1$. Of the entries in A below the diagonal nothing need be known, but it is the case, nevertheless, that A, being nilpotent, has index exactly n. For letting $e_1, \cdots, e_n$ now denote the basis of the space on which the elements of V operate, the i-th row of A is just e_iA. But then from the form of A, we have $e_1A = e_2 +$ multiple of e_1, $e_1A^2 = e_3 +$ linear combination of e_1 and e_2, etc., so that $e_1A^{n-1} = e_n +$ linear combination of e_1 to e_{n-1}; hence A^{n-1} is not zero. Therefore, if $\dim V = n(n-1)/2$, it must contain at least one element of index exactly n.

Let $N = (\nu_{ij})$ denote the matrix for which $\nu_{i,i+1} = 1$, $i = 1, \cdots, n-1$, $\nu_{ij} = 0$ for $j \neq i+1$. Then N is nilpotent of index n and is the Jordan canonical form for any $n \times n$ matrix of index n. Although usually a matrix can be transformed into Jordan canonical form only over an algebraically closed field, if A is any matrix of index n, then there exists a matrix P such that $PAP^{-1} = N$ and the elements of P are in the field of definition for A. In fact, for P, we may choose the matrix whose rows are $e_1, e_1A, \cdots, e_1A^{n-1}$, for relative to these vectors as basis, the linear transformation A has the matrix N. For the matrix A given above ($a_{i,i+1} = 1$, $i = 1, \cdots, n-1$, $a_{ij} = 0$ for $j > i+1$), the matrix P whose rows are $e_1, e_1A, \cdots, e_1A^{n-1}$ has zeros above the diagonal since the i-th row of P is $e_1A^{i-1} = e_i +$ linear combination of e_1 to e_{i-1}. Therefore $L_+(P) = L_+$, whence $L_+(P)$ is still complete, and further, $V(P) = PVP^{-1}$ contains the matrix N. We may therefore assume henceforth that L_+ is complete and that V contains N. It is then already the case, as we shall see, that V is the algebra of all $n \times n$ triangular matrices. To show this, we shall have to prove that V contains not only N but also $N^2, N^3, \cdots, N^{n-1}$.

Denoting, as before, by $s_r(M)$ the sum of the $r \times r$ principal minors of M and setting $s_r(\alpha A + B) = \alpha^{r-1}s_{r,r-1} + \cdots + \alpha s_{r,1}$, we have observed that s_{ri} is a doubly homogeneous form of degree i in the coefficients of A and of degree $r - i$ in those of B and that s_{ri} vanishes for all A and B in V. Let us set $A = (a_\sigma)$, and if σ is the pair (i, j), then σ^* will denote, as before, (j, i). Then s_{21} is a bilinear form in the elements of A and B, and a simple computation shows that $s_{21} = \sum a_{\sigma^*} b_\sigma$, the summation ranging over all pairs of indices σ. Keeping A fixed and varying B, we see that if A is in V, then a dependence relation between the vectors l_σ of the form $\sum a_{\sigma^*} l_\sigma = 0$ must hold. Let us now denote by D the set of all triangular matrices in V and by D' the set of all triangular matrices $A = (a_\sigma)$ for which $\sum a_{\sigma^*} l_\sigma = 0$ holds. Then D and D' are linear spaces, and it follows from what has just been shown that $D \subseteq D'$. If A is triangular, then $\sum a_{\sigma^*} l_\sigma = 0$ is a relation involving only those l_σ for σ in δ_-, i.e., below the diagonal, and it is clear then from the definition of D' that $\dim L_- = n(n-1)/2 - \dim D'$. But L_+ is complete and has dimension $n(n-1)/2$; therefore $\dim D = n(n-1)/2 - \dim L_+$ (for a matrix in V with zeros below the diagonal is in fact triangular). We see therefore that $\dim D = \dim D'$, whence in fact $D = D'$. Since it has been shown that V contains N, we may choose N for B, and with that choice, the s_{r1}, being linear forms in the elements of A, are easily computed. In fact, $s_{r1} = \sum a_{i+r-1,i}$, the sum ranging from $i = 1$ to $i = n - r + 1$. Since $s_{r1} = 0$ for all A in V, it is therefore the case that $\sum l_{i+r-1,i} = 0$ for $r = 1, \cdots, n$. Now for $r = 2, \cdots, n$, the pairs $(i + r - 1, i)$ are all in δ_-, and the relation $\sum l_{i+r-1,i} = 0$ is in fact equivalent to having N^{r-1} in D'. Therefore N^{r-1} is in D for $r = 2, \cdots, n$, which implies that V contains not only N but $N^2, N^3, \cdots, N^{n-1}$ as well. It follows, therefore, that if a matrix A is in V, then $A + \alpha_1 N + \cdots + \alpha_{n-1}N^{n-1}$ is nilpotent for all $\alpha_1, \cdots, \alpha_{n-1}$. But we shall show that this implies that A is actually triangular.

Suppose now that $A = (a_{ij})$ has the property that $A + \alpha_1 N + \cdots + \alpha_{n-1}N^{n-1}$ is nilpotent for all $\alpha_1, \cdots, \alpha_{n-1}$. Choosing $\alpha_i = -a_{1,j+1}$, the first row of the matrix $A + \alpha_1 N + \cdots, \alpha_{n-1}N^{n-1}$ is $(a_{11}, 0, \cdots, 0)$. Therefore, $a_{11} = 0$, else $A + \alpha_1 N + \cdots + \alpha_{n-1}N^{n-1}$ would have a non-zero latent root. Let P now be the matrix $1 + \beta_1 N + \cdots + \beta_{n-1}N^{n-1}$. Then P is non-singular and commutes with N, whence $A + \alpha_1 N + \cdots + \alpha_{n-1}N^{n-1}$ is nilpotent for all

$\alpha_1, \cdots, \alpha_{n-1}$ if and only if $PAP^{-1} + \alpha_1 N + \cdots + \alpha_{n-1} N^{n-1}$ has the same property. Therefore, for every choice of $\beta_1, \cdots, \beta_{n-1}$, the element in the first row and column of PAP^{-1} must be zero. It follows that the first column of A is zero, for choosing $\beta_i = 1$ and $\beta_j = 0$ for $j \neq i$, the element in the first row and column of PAP^{-1} is $a_{i+1,1}$. Let $e_1, \cdots, e_n$ be, as before, the basis vectors for the space $\bar{E}$ on which the matrices of V (defined now over $K(X)$) operate and let $\bar{E}'$ denote the subspace of $\bar{E}$ spanned by $e_2, \cdots, e_n$. Then it is clearly the case that $\bar{E}N$ is contained in $\bar{E}'$, and we have just shown, in effect, that $\bar{E}A$ is contained in $\bar{E}'$ also. In particular, $\bar{E}'$ is carried into itself by both N and A, and we may consider, therefore, the restrictions of N and A to this space; the matrices of these restrictions are obtained by striking out the first row and column from the matrices of N and A, respectively. Now for $n = 1$, the lemma in question is trivial, and we may therefore make the inductive assumption that it holds for all smaller values of n than the one we are considering. Stripped of its first row and column, therefore, the matrix of A is triangular; but since the first column is zero, A itself is triangular, which was to be proved.

It has therefore been shown that if V is a linear space of nilpotent $n \times n$ matrices wtih elements in a field K having at least n elements, and if $\dim V = n(n-1)/2$, then there exists a matrix which we will denote by Y such that every matrix in YVY^{-1} is triangular. If K is the field of definition for V, then Y may be taken to have coefficients in a field $K(X)$, where $X = (x_{ij})$ is a set of n^2 independent transcendental quantities over K. It was asserted, however, that one could choose for Y a matrix C with coefficients in K, and this must still be shown. Let E now denote the n-dimensional vector space over K on which the matrices of V, defined over K, operate. We must prove, in effect, that a basis can be chosen for E relative to which every matrix of V is triangular. Agreeing with the previous notation, $\bar{E}$ will denote the space obtained by extending the field of coefficients to $K(X)$. Then we have seen that $V_{K(X)}$ is similar, over $K(X)$, to the algebra of all triangular matrices. It follows, therefore, that there exists a non-zero vector in $\bar{E}$ which is annihiliated by every matrix in $V_{K(X)}$, or what is the same thing, that the intersection of the null spaces of the elements of $V_{K(X)}$ is of positive dimension. From this, it follows that the intersection of the null spaces of the elements of V (these are subspaces of E) is not zero, being in fact of the same dimension. There exists, then, a non-zero vector v in E annihiliated by every matrix of V. Let (v) denote the linear space spanned by v and E^* the quotient space $E/(v)$. Then every element A of V induces a linear transformation of E^* whose matrix is that obtained from A by deleting the last row and column. Of the $2n-1$ elements deleted from A, n are zero; hence if V^* denotes the linear space of operators on E^* so obtained, $\dim V^* \geqq n(n-)/2-(n-1)=(n-1)(n-2)/2$. Now the theorem is trivial for $n=1$, and we have $\dim E^*=n-1$. We may therefore make the inductive assumption that a basis $v_1^*,\cdots,v_{n-1}^*$ can be chosen for E^* relative to which every matrix in V^* is triangular. Then letting $v_1,\cdots,v_{n-1}$ be representatives for $v_1^*,\cdots,v_{n-1}$, v form a basis of E relative to which every matrix of V is triangular.

From the foregoing, one sees that there indeed exists a matrix C with coefficients in K such that CVC^{-1} is the algebra of all triangular matrices. It was asserted, lastly, that if A is any element of V of index exactly n, then it is sufficient to choose for C any matrix Q such that QAQ^{-1} is triangular. One may show by direct computation that if M is a triangular matrix of index n and P a non-singular matrix such that PMP^{-1} is again triangular, then P has zeros below the diagonal. Therefore, if A has index n and if Q is a matrix such that QAQ^{-1} is triangular, then Q is unique up to left multiplication by such a matrix P with zeros below the diagonal. Thus if C is a matrix such that CVC^{-1} is the algebra of all triangular matrices, then, in particular, CAC^{-1} is triangular, so $C=PQ$ for some P with zeros below the diagonal. Then $CVC^{-1}=P(QVQ^{-1})P^{-1}$, but conjugation by P carries the set of all triangular matrices onto itself, so that it must already be the case that every matrix in QVQ^{-1} is triangular. In order to effect the actual reduction of V to the set of triangular matrices, the only problem that remains is the finding of an element of index n. If $A_1,\cdots,A_k$, $k=n(n-1)/2$, is a basis for V and $x_1,\cdots,x_k$ are independent transcendentals over K, then $A(x_1,\cdots,x_k)=x_1A_1+\cdots+x_kA_k$, being a generic point of V over K, has index n, but has coefficients in $K(X)$. There must exist a specialization of $x_1,\cdots,x_k$ in K for which $A^{n-1}\neq 0$; it is therefore a finite process to find such a specialization, and this, in principle, solves the problem. Somewhat easier, perhaps, is to find a Y with coefficients in the ring $K[X]$ such that $YA(x_1,\cdots,x_n)Y^{-1}=N$. We know that there must exist a specialization of $(x_1,\cdots,x_n)$ in K over which Y and Y^{-1} have finite specializations C and C^{-1}; this gives the desired C.

Comments. The orginial motivation for the present paper is in the following theorem whose proof will be given in the second paper of this series: Let $\mathfrak{A}$ be a commutative, not necessarily associative and not necessarily finite dimensional algebra over a field of characteristic zero, and suppose there exists an integer t such that the t-th power of every element of $\mathfrak{A}$ in every association vanishes. Then the linear transformation $R_a\colon x\rightarrow xa$ of $\mathfrak{A}$ onto itself is nilpotent for every a in $\mathfrak{A}$ (in fact of index not more than $2t-3$). If $\mathfrak{A}$ is finite dimensional, then the set of right multiplications R_a, for all a in $\mathfrak{A}$, is precisely a linear space of nilpotent matrices. Unfortunately, the theorem proved here yields only meager results about such non-associative nilalgebras. A more complete description of linear varieties of nilpotent matrices would probably shed further light even on the structure of the radical of an associative algebra. It is interesting to note that there is nothing in the statement of the main theorem of this paper that involves an extension of thė the field of definition. Nevertheless, transcendental extensions, or what are in effect algebrized versions of geometric arguments, played an important role in the proof. Such arguments may be unnecessary, but it is also possible that they may prove a valuable tool in studying the structure of the radical of an algebra.

Finally, the author wishes to thank Professor Olga Taussky-Todd for ideas communicated in personal correspondence, and Professor A. A. Albert for much help and stimulation.

INSTITUTE FOR ADVANCED STUDY,
UNIVERSITY OF PENNSYLVANIA.

REFERENCE.

[1] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, New York, 1946. (Chapter II, Proposition 10.)

ON THE STRUCTURE OF LOCAL HOMEOMORPHISMS OF EUCLIDEAN *n*-SPACE, II.*

By SHLOMO STERNBERG.

1. In this paper we continue the study of local homeomorphisms of n-space begun in [6]. The main result is that every C^∞ mapping of some neighborhood of the origin onto itself, keeping the origin fixed, is equivalent via a C^∞ change of coordinates to a linear transformation, provided that a certain formal condition on the Jacobian is satisfied. If this condition is violated but no eigenvalue is of absolute value one, we show that the transformation can be brought to a simple but non-linear normal form. This result was proved in [6] for the case of contractions; the remaining cases will be treated here. In view of the connection between local mappings and differential equations (cf. Lemma 4 of [6]), our results include a C^∞ version of a well known theorem of Siegel [3] and results of Birkhoff [1] and Birkhoff and Bamforth [2]. The theorem becomes false when extended to the analytic case. In future publications we shall deal with the analytic case, and study in some detail the structure and representations of various groups of local mappings. We shall also see the true meaning of conditions (*) below in terms of the root structure of the group of all local maps.

In Section 2 we state the theorem and give a sketch of the proof in two dimensions. In Sections 3 and 4 we prove some preparatory lemmas and in Section 5 we complete the proof of the main theorem. Sections 6 and 7 are devoted to a discussion of applications and of the situation where condition (*), below, is violated.

We should like to thank Dr. Fred Brauer for many helpful conversations. Above all, we wish to thank Professor Wintner for his encouragement and advice throughout the progress of this work.

2. We now state the main theorem.

THEOREM 1. *Let T be a homeomorphism of class C^1 of $E^n \rightarrow E^n$ defined in some neighborhood of the origin, keeping the origin fixed. Let $s_1, \cdots, s_n$ be the (possibly complex or multiple) eigenvalues of $J(T)$, where $J(T)$ is the Jacobian of T at the origin. Then if*

---

* Received December 30, 1957.

(*) $s_i \neq s_1^{m_1} \cdots s_n^{m_n}$ *for all non-negative integers* $m_1, \cdots, m_n$ *with* $\sum m_i > 1$ *holds, there exist a neighborhood* N *of the origin and a function* $\lambda = \lambda(s_1, \cdots, s_n; l)$ *such that there is a change of coordinates* R *of class* λ *defined in* N *which linearizes* T. *Furthermore, for any fixed* $s_1, \cdots, s_n$, $\lambda(s_1, \cdots, s_n; l) \to \infty$ *as* $l \to \infty$. *In particular, for* $l = \infty$, R *can be chosen to be of class* C^∞.

We first observe that (*) implies that $|s_i| \neq 0, 1$ for any i. The first inequality is trivial and the second follows from the fact that since $J(T)$ is real, any eigenvalue occurs along with its complex conjugate. If we set $r_i = |s_i|^2$, we can order the r_i as

$$(1) \qquad 0 < r_1 < \cdots < r_k < 1 < r_{k+1} < \cdots < r_n.$$

For the purposes of this paper, we may assume that $0 < k < n$. In fact, if $k = n$, the mapping T is a contraction, and if $k = 0$, T^{-1} is. Both of these cases have been treated in [6]. We shall now sketch a proof of Theorem 1 for the case $n = 2$, $l = \infty$, in orded to motivate the considerations of the following sections. By Theorem 7 of [6] or Theorem 5 of [4], we can assume that the axes are invariant curves. Furthermore, (*) implies that a formal change of coordinates can be found which formally linearizes T. Choosing coordinates properly, we can then assume that T has the form

$$(\text{i}) \qquad x_1 = sx[1 + f(x,y)], \qquad y_1 = ty[1 + g(x,y)],$$

where we can assume that

$$(\text{ii}) \qquad 0 < s < 1 < t$$

and

$$(\text{iii}) \qquad f(x,y) = o((x^2+y^2)^m) \text{ and } g(x,y) = o((x^2+y^2)^m) \text{ for all } m.$$

We can also assume, by [5] or [6] Theorem 2, that $f(x,0) = g(0,y) = 0$. We then seek a change of coordinates

$$(\text{iv}) \qquad \bar{x} = x\phi(x,y), \qquad \bar{y} = y\psi(x,y)$$

which linearizes (i). Since the four quadrants are left invariant by (i), it suffices to construct ϕ and ψ in each of them and to prove that ϕ and ψ tend to 1, together with all their derivatives, as a point approaches the axis. The functional equation to be satisfied by ϕ, for example, is $sx[1 + f(x,y)]\phi(x_1,y_1) = sx\phi(x,y)$ or

$$(\text{v}) \qquad \phi(x_1,y_1) = [1 + f(x,y)]^{-1}\phi(x,y).$$

Now we can view (v) as defining ϕ at (x_1,y_1) when $\phi(x,y)$ is known. If we choose ϕ to be identically one on the line C: $y = x$, then (v) defines ϕ on the images C^n of C. If (i) were actually linear, these images would be the lines $t^{-n}y = s^{-n}x$, which tend to the axes as $n \rightarrow \pm\infty$. Since (i) doesn't differ very much from its linear part, the images C^n also approach the axes as $n \rightarrow \pm\infty$. In the case of (i) which is defined only in some small neighborhood of the origin, any point will eventually get out of N. What we mean by C^n approaching an axis is that $C^n \cap N$ does. If we call W the region bounded by C and C^1 and contained in N, we can define ϕ in W so as to be C^∞ and to be $=1$ on C and to satisfy (v) which imposes a condition only on C^1. We then define ϕ on $W^n \cap N$ as

$$\text{(vi)} \qquad \phi(x_n, y_n) = [1 + f(x,y)]^n \phi(x,y).$$

The point now is that, although n may become arbitrarily large, in order for all the images (x_k, y_k) of (x,y) to remain in N for $k \leqq n$ and n large, (x,y) must be very close to the origin; this makes $f(x,y)$ small enough to prevent any difficulty.

In the general case, no simple pre-normal form such as (i) exists and, since complex eigenvalues can enter, no '2^n-tant' need be left invariant. We can carry out the proof by replacing the half line $x = y > 0$ by the complete cone $x^2 = y^2$ or, in general, a similar cone in n dimensions.

3. In this section, we study in some detail the linear transformation L without multiple elementary divisors whose eigenvalues, s_i, satisfy (*). We first choose coordinates x_i corresponding to these eigenvalues. We then introduce the following three norms

$$\| x \|_+ = x_1^2 + \cdots + x_k^2, \qquad \| x \|_- = x_{k+1}^2 + \cdots + x_n^2,$$
$$\| x \| = \| x \|_+ + \| x \|_- = x_1^2 + \cdots + x_n^2,$$

where k is given by (1). We also introduce the cone

$$C\colon x_1^2 + \cdots + x_k^2 - x_{k+1}^2 - \cdots - x_n^2 = 0.$$

On C, $\| x \|_+ = \| x \|_- = \frac{1}{2} \| x \|$ and the complement of C consists of two open sets

$$S_+ = \{ x \mid \| x \|_+ < \| x \|_- \}$$

and

$$S_- = \{ x \mid \| x \|_- < \| x \|_+ \}.$$

It is clear that $LS_+ \subset S_+$; in fact, any point of LS_+ satisfies $\| x \|_+ / \| x \|_- \leqq r_k / r_{k+1}$. Similarly, $\bigcap_{n=0}^{\infty} L^n S_+ = I_+$, where I_+ is the subspace $I_+ = \{ x \mid \| x \|_+$

$= 0\}$. Let W denote the closed wedge $W = \overline{(S_+ - LS_+)}$; W is bounded by C and the cone

$$C_1 \colon r_1^{-1}x_1^2 + \cdots + r_k^{-1}x_k^2 - r_{k+1}^{-1}x_{k+1}^2 - \cdots r_n^{-1}x_n^2 = 0.$$

We collect these facts as

LEMMA 1. *The closure of the set* S_+ *can be decomposed into the union*

$$\bar{S}_+ = \left(\bigcup_{n=0}^{\infty} L^n W\right) \cup I_+. \tag{2}$$

For any $y \in L^m W$, *we have the inequality*

$$r_1^{m+1}/r_k^{m+1} \leqq \| y \|_+ / \| y \|_- \leqq r_k^m / r_{k+1}^m. \tag{3}$$

Now for any point x in the space,

$$r_1^m \| x \|_+ \leqq \| L^m x \|_+ \leqq r_k^m \| x \|_+ \tag{4}$$

and

$$r_{k+1}^m \| x \|_- \leqq \| L^m x \|_- \leqq r_n^m \| x \|_-. \tag{5}$$

If $x \in W$, then a consequence of (3) for $m = 0$ is

$$2 \| x \|_+ \leqq \| x \| \leqq (r_1 + r_n)/r_1 \| x \|_+ \tag{6}$$

and

$$(r_1 + r_n)/r_n \cdot \| x \|_- \leqq \| x \| \leqq 2 \| x \|_-. \tag{7}$$

If we combine (5) with (7) we obtain, for $x \in W$

$$\| L^m x \| \geqq \| L^m x \|_- \geqq \tfrac{1}{2} r_{k+1}^m \| x \|. \tag{8}$$

In particular, we have

LEMMA 2. *Let* B_r *denote the ball of radius* r *and let* $W_r = W \cap B_r$. *Then*

$$B_{\frac{1}{2}r}^+ = B_{\frac{1}{2}r} \cap S_+ \subset \bigcup_{n=0}^{\infty} (L^m W_r) \cup (I_+ \cap B_r). \tag{9}$$

If we set $W_r^m = L^m W \cap B_r$, then another consequence of (8) is that the set $L^{-m} W_r^m$ is very small for large m. More explicitly, we have

LEMMA 3. *Let* D_r^m *denote the set* $2 r_{k+1}^{-m} W_r$, *then*

$$L^{-m} W_r^m \subset D_r^m. \tag{10}$$

In particular, if $x \in L^{-m-1} W_r^{m+1}$, *then* x *can be written in the form*

$$x = r_{k+1}^{-1} x^*, \qquad x^* \in D_r^m. \tag{11}$$

Finally, if $y \in B_1^+ - I_+$, then $y = L^m x$ for some $x \in W$. We shall call x a pre-image of y. Combining (4), (6) and (8), we obtain an estimate of $\| x \|$ in terms of $\| y \|_+$, namely,

LEMMA 4. *If $y \in B_1^+ - I_+$ and if x is a pre-image of y, then*

$$\| x \|^{(1-\log r/\log r_{k+1})} \leqq (\tfrac{1}{2})^{\log r_1/\log r_{k+1}} (r_1 + r_n)/r_1 \cdot \| y \|_+. \tag{12}$$

4. In this section, we will show how to bring every C^k mapping into a prepared form so that the considerations of the following section apply. To this end, we need the following well known lemma.

LEMMA 5. *Given a real formal power series $T = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ in n variables, there exists a C^∞ function ϕ having T as its Taylor series at the origin.*

Proof. Let $\alpha(x)$ be a C^∞ *function such that* $\alpha(x) \equiv 1$ for $x < \frac{1}{4}$ and $\alpha(x) = 0$ for $x > \frac{3}{4}$. Let $M_p = \sum_p \sum_{\Sigma i_j = p} (a_{i_1 \cdots i_n})$. The the function

$$\phi = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \alpha(p! M_p \| x \|^2)$$

satisfies the requirements of the lemma.

It follows from Lemma 5 that the natural projection ϕ_k of G^k onto F^k described in [6] is onto for all k, including the case $k = \infty$. Let T be an element of G^k satisfying the hypotheses of Theorem 1. Then $\phi_k(T)$ satisfies the hypotheses of Lemma 1 of [6], and hence, since ϕ_k is onto, we can find a C^k change of coordinates so that $\phi_k(T)$ is linear in the new coordinate system. Hence, we have proved

LEMMA 6. *Let T be an element of C^l and let L be the linear approximation to T at the origin. Then, by an appropriate change of coordinates, we can arrange that $T = L + F$, where*

$$F = (f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$$

and the f's satisfy

$$f = o(\| x \|^{l/2}) \text{ if } l < \infty ; \; f = o(\| x \|^q) \text{ for all } q \text{ if } l = \infty. \tag{13}$$

If we examine the proof of Theorem 7 of [6], we see that, without destroying (11), we can arrange that I_+ and $I_- = \{x \mid \| x \|_- = 0\}$ are invariant surfaces and T reduces to the identity on I_+ and I_-. We have thus achieved the desired preliminary normalizations.

LEMMA 7. *If T satisfies the hypothesis of Theorem 1, then by a C^l*

change of coordinates it can be arranged that $T = L + F$, *where* F *satisfies* (13) *and vanishes on* I_+ *and* I_-.

5. In this section we shall complete the proof of Theorem 1. We first prove

LEMMA 8. *Let* f^* *be a* C^l *function defined on* $C_1 \cap B_r$ *and such that* f^* *satisfies* (13). *Then there exists a function* $f \in C^l$ *satisfying* (13), *defined on* W_r *and reducing to* f^* *on* C_1 *and to* 0 *on* C.

Proof. Since C_1 is a smooth retract of W, we can certainly find an f^{**} of class C^l, defined on W_r, reducing to f^* on C and satisfying (13). If α denotes the functions of § 4, the function $f = \alpha([\| x \|_+/\| x \|_-]^{\log \frac{1}{2}/\log(r_k/r_{k+1})}) f^{**}$ satisfies the requirements of the lemma, where we set $f(0) = 0$.

Proof of Theorem 1. We wish to find a change of coordinates R which satisfies the functional equation

$$RL = TR. \tag{14}$$

Now if R were defined so as to satisfy (14) on W_r, then R could be extended to $L^m W_r$ by the simple device of $R(L^m x)$ to be $T^n R(x)$. By its very definition, R would be a smooth homeomorphism on all of $\bigcup_{m=-\infty}^{\infty} L^m W$ except possibly at the origin. We shall construct an R on W_r which can be extended to all of B_ϵ for sufficiently small positive ϵ.

We define R to be the identity on C. Then the functional equation (12) imposes no condition on R in W except on C_1. In terms of coordinates, if $R(x) = x_i + g_i(x_1, \cdots, x_n)$, (14) becomes

$$g_i(Lx) = f_i(x). \tag{15}$$

We can view (15) as defining g_i, and hence R, on C_1. The g's satisfy the hypotheses of Lemma 8, so that we can extend them to all of W_r so as to vanish on C and satisfy (13). Thus, for sufficiently small r, the mapping R will be a smooth homeomorphism at all points of W_r save the origin. By the remarks above, we can extend R to be a homeomorphism on all of $B_{\frac{1}{2}r}$ with the exception of I_+ and I_-. We would like to show that R with all its derivatives approaches the identity as a point goes to I_+ or I_-. Now R is getting more and more complicated in $L^m W_r$ as $m \to \infty$. In fact, for $y = L_x{}^m$ in $L^m W_r$, we have, by (14),

$$R(L^m x) = T^m Rx = (L + F)^m Rx. \tag{16}$$

But here, Lemma 3 comes to the rescue. In fact, although the expression for R gets more involved, the x occuring in (16) gets smaller and smaller. We can formalize the situation by introducing certain function spaces as in [6]. Let G_ϵ^q be the space of all C^q mappings of the form $G = (g_1, \cdots, g_n)$, where the g_i vanish at the origin with order q, which are defined on W_ϵ. On this space, we introduce the norm

$$(17) \qquad \| G \|_\epsilon^l = \sup_{W_\epsilon} \sum_1^n \sum_{i_1+\cdots+i_n=l} (\partial g_i/\partial x_i^{i_1}\cdots\partial x_n^{i_n})^2,$$

where $l \leqq q$. It is clear that, given any $\delta > 0$ and any M, we can choose ϵ so small that

$$(18) \qquad \| G \|_\epsilon^p \leqq (\delta/nM) \| G \|_\epsilon^l, \text{ for } p < l.$$

Now let D_T denote the operator on G_ϵ^q given by

$$(19) \qquad D_T\colon G(\cdot) \rightarrow (L+F)(E+G)(\cdot\, r_{k+1}^{-1}\cdot) - L \cdot r_{k+1}^{-1}.$$

Then, since G admits a factor of $\| x \|^q$ and we can choose δ as small as we please, we have, given any α, for sufficiently large q,

$$(20) \qquad \| D_T^G \|_\epsilon^l \leqq \alpha \| G \|_\epsilon^l + \| F \|_\epsilon^l.$$

In particular, we can choose $\alpha < r_n^{-l}$. Then, by Lemma 3, (16) and (20), we have that R approaches the identity with its first l derivatives as $m \rightarrow \infty$ if q is sufficiently large. Thus, at any point of I_+ and I_- other than the origin, R is of class C^l. At the origin, we can assume that the approach to the origin is through points of $L^m W^r$ with m bounded, since, for $M \rightarrow \infty$, $R \rightarrow E$. But then the estimates of Lemma 4 apply, since the expression for R is of one of a finite number of forms. Thus R can be defined on all of B_r, proving Theorem 1.

6. It should be noted that the estimates occurring in the proof of Theorem 1 depend, really, only on the ratios of the r_i. Thus, by Lemma 4 of [6], if T_t is a continuous one parameter group of transformations, it can be linearized provided the eigenvalues of a Jacobian (and hence of all Jacobians) at the origin satisfy (*). If we apply the considerations of Section 7 of [6], we obtain the following theorem on differential equations (which we state for, simplicity, in the C^∞ case).

THEOREM 2. *Let the system of differential equations*

$$(21) \qquad dx_i/dt = X_i(x_1, \cdots, x_n)$$

be C^∞ *and such that* $X_i(0,\cdots,0)=0$. *Let* λ_i *denote the eigenvalues of the matrix of linear terms of the* X_i. *Then if*

$$(**)\qquad \lambda_i \neq m_i\lambda_i \textit{ for any positive integral } m_i \textit{ with } m_i > 1,$$

there exists a C^∞ *change of coordinates linearizing* (21).

This theorem is the C^∞ version of a well known result of Siegel [3]. It also generalizes to n dimensions the results of Birkhoff [1] in two dimensions and Birkhoff and Bamforth [2] for real eigenvalues in three dimensions, without their unnatural analyticity requirements.

7. In this section we wish to consider what happens when (*) is violated. We still retain, however, condition (1). In fact, if (1) were violated and some eigenvalue were of absolute value one, then the linear term is stable (on some lower dimensional invariant surface) and cannot be indicative of what happens in the non-linear case. We also note that the considerations of § 3 apply to non-linear as well as to linear transformations, provided that a small modification is made in all of the constants occurring in the lemmas. We shall asume, for simplicity, that the eigenvalues s_i are real; complex eigenvalues add no essential difficulties. Let M_i denote the set of n-tuples of positive integers $(m_1,\cdots,m_n)$ such that

$$(22)\qquad s_i = s_i^{m_1}\cdots s_n^{m_n}.$$

If m and m^* are two elements of M_i, then $m - m^* \in S$, where S is the group of those n-tuples $(m^1,\cdots,m_n)$ such that

$$(23)\qquad 1 = s_1^{m_1}\cdots s_n^{m_n}.$$

Then choosing a basis B for the positive elements of S, we can express all but a finite number of elements of M_i as products of some one element m and multpiles of elements of B. Combining these considerations with Lemma 9 of [6] and Lemma 5 above, we obtain

THEOREM 3. *Let* T *be a* C^∞ *local mapping whose eigenvalues at the origin satisfy* (1). *Then there exist a finite number of monomials depending only on the eigenvalues, such that* T *is equivalent to a transformation of the form* $L+F$, *where* L *is linear and* F *depends only on the* P_j*'s.*

For example, if $n=2$ and $s_1 = s_2^{-1}$, we can find a change of coordinates so that T has the form

$$x_1 = sx + xf(xy), \qquad y_1 = s^{-1}y + yg(xy).$$

THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] G. D. Birkhoff, " Divergente Reihen und singuläre Punkte gewöhnlicher Differentialgleichungen," *Berliner Sitzungsberichte der Preussischen Akademie der Wissenschaften,* 1929, pp. 1-15.

[2] ——— and F. R. Bamforth, " Divergent series and singular points of ordinary differential equations," *Transactions of the American Mathematical Society,* vol. 32 (1930), pp. 114-146.

[3] C. L. Siegel, " Über die Normalform analytischer Differentialgleichungen in der Nähe einer Gleichgewichtslösung," *Göttinger Nachrichten der Akademie der Wissenschaften,* 1952, pp. 21-30.

[4] S. Sternberg, " On the behavior of invariant curves near a hyperbolic point of a surface transformation," *American Journal of Mathematics,* vol. 75 (1955), pp. 526-534.

[5] ———, " On local C^n contractions of the real line," *Duke Mathematical Journal,* vol. 24 (1957), pp. 97-102.

[6] ———," Local contractions and a theorem of Poincaré," *American Journal of Mathematics,* vol. 79 (1957), pp. 809-824.

ON THE PONTRYAGIN CLASSES OF CERTAIN $SO(n)$-BUNDLES OVER MANIFOLDS.*

By MICHEL A. KERVAIRE.

One of the main steps in the proof of the well known

THEOREM (Rochlin [4]). *If* $w_2(M_4) = 0$, *then* $p_1(M_4)$ *is divisible by* 48, is the following lemma due to Pontryagin who stated it without proof in the Doklady Akademii Nauk S.S.S.R., XLVII, N. 5, pp. 327-330. (In Rochlin's theorem, $w_2(M_4)$ is the 2-dimensional Stiefel-Whitney class of the 4-dimensional, orientable, closed, differentiable manifold M_4 and $p_1(M_4)$ the first (4-dimensional) Pontryagin class of M_4.)

LEMMA. *Let the closed differentiable manifold* M_4 *of dimension* 4 *be the base space of a principal* $\boldsymbol{SO}(n)$*-bundle* $\mathfrak{N}$. *Assume that* $\mathfrak{N}$ *admits a cross-section over the subset* $M - U$ *of* M, *where* U *is a spherical neighborhood of some point in* M_4. *Let* $\lambda \in \pi_3(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$ *be the integer representing, up to sign, the obstruction to the extension over* M *of the cross-section given over* $M - U$. *Then,* $p_1(M_4) = 2\lambda$, *up to sign.*

A tentative method toward generalizing Rochlin's theorem starts with generalizing this lemma. This is done below. I do not know whether this will actually lead to a reasonable generalization of Rochlin's theorem. However, the generalized lemma might have some interest in itself.

I am indebted to A. Borel for valuable discussions during the preparation of the present paper.

1. Let M_{4s} be a closed manifold of dimension $4s$. Let $\mathfrak{N}$ be a principal $\boldsymbol{SO}(n)$-bundle over M_{4s} which admits a cross-section over $M - U$. We shall say for brevity that the bundle $\mathfrak{N}$ is "*almost trivial.*" Assume that $4s < n$ and let λ denote the integer representing the homotopy class in $\pi_{4s-1}(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$ (see [1]) of the obstruction to the extension over M_{4s} of the cross-section given over $M - U$. All manifolds considered in this paper are assumed to be orientable.

---

* Received January 10, 1958.

LEMMA (1.1). *The value on* M_{4s} *of the* $4s$*-dimensional Pontryagin class* p_s *of the bundle* $\mathfrak{N}$ *is given by the formula:* $p_s[M_{4s}] = a_s \cdot \lambda \cdot (2s-1)\,!$, *up to sign, where* a_s *is equal to* 1 *or* 2 *according to whether* s *is even or odd respectively.*

Results concerning the same question in the non-stable range ($n < 4s+1$) can be deduced (using Lemma (3.1) below) from results in a forthcoming paper by A. Borel and F. Hirzebruch: "On the characteristic classes of homogeneous spaces."

Before we proceed to the proof of the above lemma, let us recall briefly the argument by which it implies Rochlin's theorem:

2. Let the orientable, closed, differentiable manifold M_4 be imbedded in euclidean $(n+4)$-space E_{n+4} in such a way that U is the hemisphere $x_0 \leqq 0$ of the unit sphere $S_4 \subset E_5 \subset E_{n+4}$. Assume that $M - U$ lies in $\{x_0 \geqq 0\}$ and that the imbedding of M_{4s} in E_{n+4} is differentiable of class C^2. The assumption $w_2(M_4) = 0$ is equivalent to the existence of a field of n-frames $\boldsymbol{F}_n$ defined over $M - U$ and orthogonal to M_4 in E_{n+4} (because M_4 was assumed to be orientable and $\pi_2(\boldsymbol{SO}(n)) = 0$). By Lemma (1.1), $\bar{p}_1[M_4] = 2\lambda$, where $\bar{p}_1$ is the 4-dimensional Pontryagin class of the normal bundle over M_4 in E_{n+4}. The integer λ represents the homotopy class of the mapping $\mu\colon S_3 \rightarrow \boldsymbol{SO}(n)$ which sends a point $x \in U^{\cdot}$ (identified with S_3) into the matrix of components of the vectors of $\boldsymbol{F}_n$ at x relative to the vectors at x of some field of normal n-frames over S_4 in E_{n+4} (Take for instance the field consisting of the normal to S_4 in E_5 followed by the vectors of an orthonormal basis of the orthogonal complement of E_5 in E_{n+4}). By the interpretation of J (the Hopf's homomorphism) given in [2] and the fact that $\boldsymbol{F}_n \mid U^{\cdot}$ can be extended over $M - U$, it follows that the element $J\mu \in \pi_{n+3}(S_n)$ is zero. Since $J\pi_3(\boldsymbol{SO}(n)) = \pi_{n+3}(S_n) \approx \boldsymbol{Z}_{24}$, it follows that λ is divisible by 24. Consequently $\bar{p}_1[M_4]$ is divisible by 48. By Whitney duality (which holds over the integers in this special case), we have $p_1[M_4] = -\bar{p}_1[M_4]$. Hence the theorem.

3. Using the following lemma, we reduce the study of almost trivial bundles over a closed manifold M_d to the study of bundles over the sphere S_d:

LEMMA (3.1). *Let* $f\colon M_d \rightarrow B_G$ *be a mapping of* M_d *into the classifying space for* G *and assume that the induced principal* $\boldsymbol{G}$*-bundle over* M_d *is almost trivial* (i.e., *admits a cross-section over* $M - U$). *Then* f *is homo-*

topic to a composite map $f' \circ \alpha$, *where* $\alpha\colon M_d \to S_d$ *has degree* 1 *and* f' *maps* S_d *into* B_G.

Proof of lemma (3.1). Denote by $\pi\colon E_G \to B_G$ the projection in the classifying fibration. Since the bundle over M_d induced by f is almost trivial, there exists a mapping $F\colon M - U \to E_G$, such that $\pi \circ F = f \mid M - U$. We may assume that f is constant on U: $f(U) = b \in B_G$. The map F is homotopic to zero (E_G is contractible). Let F_t be a homotopy: $F_0 = F$, F_1 maps $M - U$ into some points of E_G. It is convenient for later purposes to assume that $F_t = F$ for $0 \leqq t \leqq \frac{1}{2}$. Introduce generalized polar coordinates (x, r) in U ($x \in U^{\cdot}$, $r =$ distance from (x, r) to the center of U). The required homotopy between f and a map of the form $f' \circ \alpha$ is given by

$$f_t(z) = \pi F_t(z) \qquad \text{for } z \in M - U,$$

$$f_t(x, r) = \pi F_{tr}(x, 1) \quad \text{for } (x, r) \in U$$

(We take the radius of U to be 1).

Clearly, $f_t(z)$ is continuous in both z *and* t. We verify that $f_0 = f$: for

$z \in M - U$, $f_0(z) = \pi F_0(z) = \pi F(z) = f(z)$; for

$$(x, r) \in U,\ f_0(x, r) = \pi F_0(x, 1) = \pi F(x, 1) = f(x, 1) = f(x, r) = b.$$

For $t = 1$, we have

$$f_1(z) = \pi F_1(z) = b' \text{ a constant point } (z \in M - U),$$

$$f_1(x, r) = \pi F_r(x, 1).$$

Clearly, f_1 has the form $f' \circ \alpha$, where $\alpha\colon M_d \to S_d$ shrinks $M - U$ into a point and maps the interior of U homeomorphically into S_d (thus α has degree 1), and f' sends $\alpha(x, r)$ into $\pi F_r(x, 1)$.

4. Let $f\colon M_{4s} \to B_{SO(n)}$ induce an almost trivial bundle over M_{4s} ($4s + 1 < n$). We may assume, without loss of generality, that the section over $M - U$ is given by a mapping $F\colon M - U \to E_{SO(n)}$ (such that $\pi F = f \mid M - U$). Assuming for convenience as in § 3 that $f(U) = b \in B_{SO(n)}$, $F \mid U^{\cdot}$ defines a mapping of S_{4s-1} into $\boldsymbol{SO}(n)$. Since we assumed $4s + 1 < n$, one has by [1], $\pi_{4s-1}(\boldsymbol{SO}(n)) \cong \boldsymbol{Z}$. Let λ be the integer (determined up to sign) representing the homotopy class of $F \mid U^{\cdot}$ in $\boldsymbol{SO}(n)$. Denote by

$p_s \in H^{4s}(M_{4s}; \boldsymbol{Z})$ the Pontryagin class of dimension $4s$ of the $\boldsymbol{SO}(n)$-bundle over M_{4s} induced by f. We have to prove that $p_s[M_{4s}] = a_s \cdot \lambda \cdot (2s-1)\,!$.

Let $f' \circ \alpha \simeq f$ be the factorization given by Lemma (3.1). Denote by χ the characteristic map of the bundle over S_{4s} induced by f'. We shall prove (up to sign):

(1) $\chi = \lambda$, (we use also χ to denote the integer representing the homotopy class of χ),

(2) $p_s[M_{4s}] = p'[S_{4s}]$, where p'_s is the $4s$-dimensional Pontryagin class of the bundle over S_{4s} induced by f'.

(3) $p'_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)\,!$.[1]

Proof of (1). Define $F' : {}_\bullet S_{4s} - V \rightarrow E_{\boldsymbol{SO}(n)}$ by $F'(\alpha(x,r)) = F_r(x,1)$, where V is the image by α of the set of those $(x,r) \in U$ with $0 \leqq r \leqq \frac{1}{2}$. Since we assumed $F_t = F$ for $0 \leqq t \leqq \frac{1}{2}$ (see § 3), $\pi F'(V^{\cdot}) = \pi F(U_{\frac{1}{2}}^{\cdot}) = f(U_{\frac{1}{2}}^{\cdot}) = b$, where $U_{\frac{1}{2}}^{\cdot}$ is the set of points $(x, \frac{1}{2}) \in U$. On the other hand, $\pi F' = f' \mid S_{4s} - V$. In other words, $F' \mid V^{\cdot}$ defines a mapping $S_{4s-1} \rightarrow \boldsymbol{SO}(n)$ which is precisely the characteristic map χ of the bundle over S_{4s} induced by f' (we use χ for the map and its homotopy class). But $F'(x, \frac{1}{2}) = F_{\frac{1}{2}}(x,1) = F(x,1)$. This means that χ is also represented by $F \mid U^{\cdot}$. Hence $\chi = \lambda$.

Proof of (2). Trivial by naturality of the Pontryagin classes (and the fact that α has degree 1).

Proof of (3). We are left with the following situation: Let $(E, \boldsymbol{SO}(n), S_{4s})$ be a principal $\boldsymbol{SO}(n)$-bundle over S_{4s} and χ its characteristic map. $\chi = \partial i_{4s}$, where ∂ is the boundary operator in the homotopy sequence of $\pi : E \rightarrow S_{4s}$. Let p_s be the $4s$-dimensional Pontryagin class of $(E, \boldsymbol{SO}(n), S_{4s})$. We have to prove:

$$p_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)\,!$$

(up to sign).

Let $\alpha : \boldsymbol{SO}(n) \rightarrow \boldsymbol{U}(n)$ be the standard injection and denote by c_{2s} the $4s$-dimensional Chern class of the extended bundle $(E', \boldsymbol{U}(n), S_{4s})$. By definition $p_s[S_{4s}] = c_{2s}[S_{4s}]$ up to sign. It is well known that $\pi_{4s-1}(W_{n,n-2s+1}) \approx \boldsymbol{Z}$. We have $\partial_A i_{4s} = c_{2s}[S_{4s}] \cdot \epsilon_W$, where $\partial_A : \pi_{4s}(S_{4s}) \pi_{4s-1}(W_{n,n-2s+1})$ is the boundary operator of the homotopy sequence of the fibration with fibre $W_{n,n-2s+1}$ associated with $(E', \boldsymbol{U}(n), S_{4s})$ and ϵ_W is a generator of $\pi_{4s-1}(W_{n,n-2s+1})$.

To evaluate $c_{2s}[S_{4s}]$, consider the commutative diagram

---

[1] The divisibility of $p'_s[S_{4s}]$ by $(2s-1)\,!$ is also known to R. Bott.

$$\begin{tikzcd}
\pi_{4s-1}(\boldsymbol{SO}(n)) \arrow[r, "\alpha_*"] & \pi_{4s-1}(\boldsymbol{U}(n)) \arrow[r, "q_*"] & \pi_{4s-1}(W_{n,n-2s+1}) \\
\pi_{4s}(S_{4s}) \arrow[u, "\partial"'] \arrow[r, "\text{identity}"] & \pi_{4s}(S_{4s}) \arrow[u] \arrow[r, "\text{identity}"] & \pi_{4s}(S_{4s}), \arrow[u, "\partial_A"']
\end{tikzcd}$$

where $q\colon \boldsymbol{U}(n) \to W_{n,n-2s+1}$ is the natural projection. Using the definition of $c_{2s}[S_{4s}]$, we get

$$c_{2s}[S_{4s}] \cdot \epsilon_W = \partial_A(i_{4s}) = q_* \alpha_* \partial(i_{4s}) = \chi q_* \alpha_* \epsilon_{SO} = a_s \cdot \chi \cdot q_* \epsilon_U,$$

where χ denotes also the integer representing the homotopy class of χ.

Consider the homotopy sequence of the fibration $\boldsymbol{U}(n)/\boldsymbol{U}(2s-1) = W_{n,n-2w+1}$ with projection q:

$$\cdots \to \pi_{4s-1}(\boldsymbol{U}(n)) \longrightarrow \pi_{4s-1}(W_{n,n-2s+1}) \to \pi_{4s-2}(\boldsymbol{U}(2s-1)) \to \pi_{4s-2}(\boldsymbol{U}(n)).$$

By R. Bott, $\pi_{4s-2}(\boldsymbol{U}(n)) = 0$ and $\pi_{4s-2}(\boldsymbol{U}(2s-1)) = \boldsymbol{Z}/(2s-1)!\boldsymbol{Z}$. Therefore, q_* is the multiplication by $(2s-1)!$ (precisely, $q_*\epsilon_U = (2s-1)!\epsilon_W$). It follows that

$$p_s[S_{4s}] = a_s \cdot \chi \cdot (2s-1)!,$$

up to sign. It was proved in [3], Lemma 3, that $a_{2k+1} = 2$ and $a_{2k} = 1$. This completes the proof of Lemma (1.1).

5. *Remarks.* The same method gives the Chern class c_s of an almost trivial $\boldsymbol{U}(n)$-bundle over a $2s$-dimensional manifold ($s \leqq n$) and similarly the symplectic Pontryagin class e_s of an almost trivial $\boldsymbol{Sp}(n)$-bundle over a $4s$-dimensional manifold (for the "symplectic" Pontryagin classes, see A. Borel and F. Hirzebruch, loc. cit., Chapter I, 9.6).

LEMMA (5.1). *Let M_{2s} be the base space of an almost trivial principal $\boldsymbol{U}(n)$-bundle $\mathfrak{N}$. Let $\lambda(F)$ be the obstruction to the extension M_{2s} of a cross-section F in $\mathfrak{N}$ given over $M - U$ ($\lambda(F) \in \pi_{2s-1}(\boldsymbol{U}(n))$). Assume $s < n$, thus $\pi_{2s-1}(\boldsymbol{U}(n)) \approx \boldsymbol{Z}$. Let c_s denote the $2s$-dimensional Chern class of $\mathfrak{N}$. We have $c_s[M_{2s}] = (s-1)!\lambda(F)$.*

Similarly, let M_{4s} be the base space of an almost trivial $\boldsymbol{Sp}(n)$-bundle $\mathfrak{N}$. Assume $s < n$, then the obstruction to the extension over M of a cross-section defined over $M - U$ (U some spherical neighborhood in M) can be represented by an integer $\lambda(\pi_{4s-1}(\boldsymbol{Sp}) \approx \boldsymbol{Z}$ by R. Bott [1]). Let σ be the standard inclusion $\sigma\colon \boldsymbol{Sp}(n) \to \boldsymbol{U}(2n)$ and $\sigma^*\colon H^*(B_{U(2n)}) \to H^*(B_{Sp(n)})$ the induced homomorphism in integral cohomology of the classifying spaces. The symplectic Pontryagin classes of an $\boldsymbol{Sp}(n)$-bundle induced by a mapping $f\colon M \to B_{Sp(n)}$ are, up to sign, the images by $f^* \circ \sigma^*$ of the universal Chern classes $C_{2i} \in H^{4i}(B_{U(2n)})$.

LEMMA (5.2). *Let e_s denote the 4s-dimensional symplectic Pontryagin class of $\mathfrak{N}$. We have $e_s[M_{4s}] = b_s \cdot \lambda \cdot (2s-1)\,!$, where b_s is equal to 1 if s is odd, to 2 if s is even.*

The proofs are entirely similar to the one of Lemma (1.1) and are left to the reader. For the proof of Lemma (5.2), one has to use that $\sigma_*\colon \pi_{4s-1}(\boldsymbol{Sp}(n)) \to \pi_{4s-1}(\boldsymbol{U}(2n))$ maps a generator into b_s-times a generator, a fact which follows from [1], formula (3.6) and the knowledge of the stable homotopy groups of $\boldsymbol{Sp}(n)$.

We have two more remarks: in the situations of Lemmas (1.1), (5.1) and (5.2), it follows that $\lambda(F)$, the obstruction to the extension of the partial cross-section F, does not depend on F, a fact which could also be proved directly (the Hurewicz homomorphisms

$$\pi_{2s-1}(\boldsymbol{U}(n)) \to H_{2s-1}(\boldsymbol{U}(n)), \qquad \pi_{4s-1}(\boldsymbol{SO}(n)) \to H_{4s-1}(\boldsymbol{SO}(n)),$$
$$\pi_{4s-1}(\boldsymbol{Sp}(n)) \to H_{4s-1}(\boldsymbol{Sp}(n))$$

are monomorphisms[2] for large n).

Finally, we notice that R. Bott's result: $\pi_{2n}(\boldsymbol{U}(n)) \approx \boldsymbol{Z}/n\,!\boldsymbol{Z}$ which was used in both Lemmas (1.1) and (5.2) implies

(5.3) $\quad \pi_{4s-2}(\boldsymbol{Sp}(s-1)) \approx \boldsymbol{Z}/b_s(2s-1)\,!\boldsymbol{Z}$. ($b_s$ as in Lemma (5.2)).

Indeed, the projection k_* in the homotopy sequence

$$\cdots \to \pi_{4s-1}(\boldsymbol{Sp}(s)) \xrightarrow{k_*} \pi_{4s-1}(S_{4s-1}) \to \pi_{4s-2}(\boldsymbol{Sp}(s-1)) \to \pi_{4s-2}(\boldsymbol{Sp}(s))$$

is the composition $k_* = q_* \circ \sigma_*$, where $\sigma_*\colon \pi_{4s-1}(\boldsymbol{Sp}(s)) \to \pi_{4s-1}(\boldsymbol{U}(2s))$ is induced by the standard inclusion $\sigma\colon \boldsymbol{Sp}(s) \to \boldsymbol{U}(2s)$ and $q_*\colon \pi_{4s-1}(\boldsymbol{U}(2s)) \to \pi_{4s-1}(S_{4s-1})$ is induced by the projection $q\colon \boldsymbol{U}(2s) \to S_{4s-1}$. Now, σ_* sends generator into b_s-times generator and q_* sends generator into $(2s-1)\,!$-times generator. Therefore, k_* sends a generator of $\pi_{4s-1}(\boldsymbol{Sp}(s)) \approx \boldsymbol{Z}$ into $b_s \cdot (2s-1)\,!$ times a generator of $\pi_{4s-1}(S_{4s-1})$. Since $\pi_{4s-2}(\boldsymbol{Sp}(s)) = 0$, we have $\pi_{4s-2}(\boldsymbol{Sp}(s-1)) \approx \pi_{4s-1}(S_{4s-1})/k_*\pi_{4s-1}(\boldsymbol{Sp}(s))$. Hence (5.3).

THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] R. Bott, "The stable homotopy of the classical groups," *Proceedings of the National Academy of Sciences*, vol. 43 (1957), pp. 933-935.

[2] M. Kervaire, "An interpretation of G. Whitehead's generalization of Hopf's invariant," to appear.

[3] ———, "Non-parallelizability of S_n for $n > 7$," *Proceedings of the National Academy of Sciences*, vol. 44 (1958), pp. 280-283.

[4] W. Rochlin, "Classification of mappings of S_{n+3} onto S_n," *Doklady Akademii Nauk S.S.S.R.*, vol. 81 (1951).

ON THE λ-VARIANT OF MERTENS' μ-HYPOTHESIS.*

By Aurel Wintner.

Let $M(n)$, $L(n)$; $J(n)$, $K(n)$ denote the n-th partial sums of the series $\Sigma\mu(n)$, $\Sigma\lambda(n)$; $\Sigma\mu(n)/\sqrt{n}$, $\Sigma\lambda(n)/\sqrt{n}$ respectively, where $\mu(n)$ and $\lambda(n)$ are Möbius' and Liouville's factors, defined by $1/\zeta(s) = \Sigma\mu(n)/n^s$ and $\zeta(2s)/\zeta(s) = \Sigma\lambda(n)/n^s$. According to Littlewood, the convergence of either (or both) of the latter series for $s > \frac{1}{2}$ is equivalent to Riemann's hypothesis ($=$R. H.). According to Landau, the unilateral boundedness of any one of the functions $M, \cdots, K$ of n implies, without being implied by, R. H. In particular, more than R. H. is implied (for trivial reasons) not only by Mertens' hypothesis

$$(1) \qquad M(n) = O(\sqrt{n}), \quad \text{where } M(n) = \sum_{m=1}^{n} \mu(m),$$

but also by Pólya's hypothesis ($=$P. H.), which claims that $L(n) \leqq 0$ (or even $L(n) < 0$) holds for every $n > 1$ (or $n > 2$) ; for references and certain conclusions cf. a paper of Ingham [1] (and, concerning a λ-hypothesis which is distinct from P. H. and was propounded by Turán, the recent conclusions of S. Selberg [2].

Neither the necessity nor the sufficiency of (1) for P. H. is known (and, what is more curious, no implicative connection is known between Pólya's and Turán's λ-hypotheses). On the other hand, the formal λ-analogue of (1) is not P. H. but

$$(2) \qquad L(n) = O(\sqrt{n}), \quad \text{where } L(n) = \sum_{m=1}^{n} \lambda(m).$$

I do not know of an implicative connection between either (1) or P. H. (or, for that matter, S. Selberg's version of Turán's hypothesis) on the one hand, and the hypothesis (2), which does not seem to have been considered in the literature, on the other hand. But something *like* P. H. (a certain "negative preponderance" of the same type as P. H.) can be expected to follow from (2), and even from R. H., which claims less than (2). Such an expectation rests on the circumstance that

$$(3) \qquad \operatorname*{res}_{s=\frac{1}{2}} \zeta(2s)/\zeta(s) < 0.$$

---

* Received May 14, 1958.

As a matter of fact, the available numerical evidence for the truth of P. H. could be *merely a reflection of* (3). [Needless to say, (3) follows not only from the value of $\zeta(\frac{1}{2})$ but, more immediately, from the circumstance that, whereas $\zeta(2s)$ does not change sign when s passes from $s > 1$ to $s < 1$, the function $\zeta(s)$, having a *simple* pole at $s = 1$, must change sign at $s = 1$ on the real axis.]

Actually, while (3) does not seem to be able to lead from (2) to a "negative preponderance" in terms of $L(n)$ (which is P. H.), it does lead to a "negative preponderance" in terms of $K(n)$. In fact, (2) turns out to imply that

$$(4) \qquad K(n)/\log n \to c, \quad \text{where } K(n) = \sum_{m=1}^{n} \lambda(m)/\sqrt{m},$$

holds for a certain *negative* constant c, and so $K(n) \to -\infty$. But much more than (4) can be concluded if an argument applied to (1) in an earlier note [3] is adapted to (2).

Consider the following refinement (1*) of (1):

$$(1^*) \qquad J(n) = O(1), \quad \text{where } J(n) = \sum_{m=1}^{n} \mu(m)/\sqrt{m}.$$

A partial summation shows that (1*) implies (1). On the other hand, a partial summation fails to lead from (1) to (1*). In fact,

$$[\sum_{m=1}^{n} c_m = O(\sqrt{n})] \Rightarrow [\sum_{m=1}^{n} c_m/\sqrt{m} = O(\log n)]$$

for arbitrary $c_1, c_2, \cdots$ but, as shown by the example $c_n = 1/\sqrt{n}$, nothing more can in general be concluded. But the $O(\log n)$ can be improved to $O(1)$ in the particular case $c_n = \mu(n)$, which means that (1) is equivalent to (1*). As shown in [3], this follows for function-theoretical Tauberian reasons. Since the truth of (1*) appears to be quite unlikely (it may or, in contrast with (1), it may not at all, be indicated by the beginning of a numerical table), the usual "theoretical" objection against Mertens' hypothesis appears in a strengthened form.

It turns out that the "theoretical" objection to (2) can be straightened correspondingly, and in a manner which appears to be even more striking (though actually it is not). In fact, *the following relation* (2*) *proves to be equivalent to* (2):

$$(2^*) \qquad K(n) = c \log n + O(1), \quad \text{where } K(n) = \sum_{m=1}^{n} \lambda(m)/\sqrt{m}$$

(here c denotes, as in (4), a certain negative constant). This speaks much against (2), since the truth of anything like (2*) seems to be unlikely.

Proof of $(2^*) \Rightarrow (2)$. This requires nothing but a partial summation (no matter what the given value of c may be).

Proof of $(2) \Rightarrow (2^*)$. In [3], the proof of $(1) \Rightarrow (1^*)$ resulted, on the one hand, from the fact that

(i) the function $1/\zeta(s)$ is regular at the point $s = \frac{1}{2}$, and, on the other hand, from an application of

(ii) a lemma Tauberian in nature, representing an *O-variant* of M. Riesz' *convergence* theorem concerning Dirichlet series (the convergence theorem which extends Fatou's theorem on power series to Dirichlet series).

Condition (i) becomes violated if the function $1/\zeta(s)$, occurring in (i), is replaced by the function $\zeta(2s)/\zeta(s)$, since the latter has a pole at $s = \frac{1}{2}$. This pole can, however, be eliminated if $\zeta(2s)/\zeta(s)$ is replaced by the sum $\gamma(s)$ defined by

$$\gamma(s) = \zeta(2s)/\zeta(s) - c\zeta(s + \tfrac{1}{2}), \tag{5}$$

where c is a constant, to be determined by the condition that the simple pole possessed at $s = \frac{1}{2}$ by the first term of (5) be compensated by the simple pole possessed at $s = \frac{1}{2}$ by the second term of (5). Accordingly, condition (i) is satisfied if the function $1/\zeta(s)$ is replaced by the function (5), where $c < 0$, by (3).

Since

$$\zeta(2s)/\zeta(s) = \sum_{n=1}^{\infty} \lambda(n)/n^s \text{ and } \zeta(s) = \sum_{n=1}^{\infty} 1/n^s,$$

it is seen from (5) that the series

$$1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n)/n^s \tag{6}$$

must be replaced by the series

$$\gamma(s) = \sum_{n=1}^{\infty} [\lambda(n) - c/\sqrt{n}]/n^s. \tag{7}$$

But what corresponds to the hypothesis (1) for the Dirichlet series (6) is the hypothesis

$$\sum_{m=1}^{n} [\lambda(m) - c/\sqrt{m}] = O(\sqrt{n}) \tag{8}$$

for the Dirichlet series (7). Consequently, if the Tauberian lemma, referred to under (ii), is used in precisely the same way as it was used in the proof of $(1) \Rightarrow (1^*)$ in [3], then, since what now corresponds to (1^*) is the estimate

$$\sum_{m=1}^{\infty} [\lambda(m) - c/\sqrt{m}]/\sqrt{m} = O(1), \tag{9}$$

there results the truth of the (unconditional) implication $(8) \Rightarrow (9)$.

Finally,

$$\sum_{m=1}^{n} 1/\sqrt{m} = O(\sqrt{n}) \text{ and } \sum_{m=1}^{n} (c/\sqrt{m})/\sqrt{m} = c \log n + O(1)$$

(the $O(1)$ claims less than the existence of the Euler-Mascheroni constant). Hence, (8) and (9) are equivalent to (2) and (2^*) respectively. Consequently, $(8) \Rightarrow (9)$ is equivalent to $(2) \Rightarrow (2^*)$. Since $(8) \Rightarrow (9)$ was just proved, the proof of $(2) \Rightarrow (2^*)$ is complete.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] A. E. Ingham, "On two conjectures in the theory of numbers," *American Journal of Mathematics*, vol. 64 (1942), pp. 313-319.

[2] S. Selberg, "Über eine Vermutung von P. Turán," *Det Kongelige Norske Videnskabers Selskabs Forhandlinger*, vol. 29 (1956), pp. 33-35.

[3] A. Wintner, "A note on Mertens' hypothesis," *Revista de Ciencias* (Lima), vol. 50 (1948), pp. 181-184.

PARTITIONS OF LARGE BIPARTITES.*

By E. M. WRIGHT.

1. In a recent article [4], I found an asymptotic formula for the number of partitions of a bi-partite number (m, n) whose components m, n are large but of the same order, i. e., their ratio is bounded above and below. I also gave without proof the first few terms of an asymptotic formula for the logarithm of the number of partitions of a multi-partite number $(n_1, n_2, \cdots, n_j)$, the ratios of whose components are all bounded below. Just before the article appeared, I found that Auluck [1] had dealt with one of my four cases for bipartites, under the same condition, and that Meinardus [2] had found the first term of my formula for multi-partites. Auluck indicates that his results for bi-partites (and any results obtainable for multi-partites) have applications to the study of the thermodynamical properties of assemblies characterised by the conservation of two or more parameters. He found an entirely different result true when m is fixed and n large, and Nanda [3] has shown that this is true for $m = o(n^{\frac{1}{4}})$.

A much more precise approximation for the generating function has now been found [6], and this enables me to deal here with all large m and n such that

$$\frac{1}{2} + \epsilon_1 < \log n / \log m < 2 - \epsilon_2 \tag{1.1}$$

for any fixed positive ϵ_1, ϵ_2. This is a substantial relaxation of the restriction imposed in both [1] and [4] that m/n should be bounded above and below.

Auluck's result and the result in two of my four cases involved a definite integral $I(m/n)$ which neither of us was then able to evaluate (except that Auluck evaluated $I(1)$). This problem has since been solved [5], and I use the results here.

2. Notation and Result. A *bi-partite number* (m, n) is a two-dimensional vector whose components m, n are non-negative rational integers. A *partition* of (m, n) is a solution of the vector equation

$$\sum_k (m_k, n_k) = (m, n) \tag{2.1}$$

---

* Received January 6, 1958.

in bi-partite numbers other than $(0,0)$; two partitions are regarded as identical if they differ only in the order of the bi-partite numbers on the left of (2.1). We write $p^{(1)}(m,n)$ for the number of partitions of (m,n) and $p^{(2)}(m,n)$ for the number of such partitions in which no part has a zero component. Again, we write $p^{(3)}(m,n)$ for the number of partitions of (m,n) into *different* parts and $p^{(4)}(m,n)$ for the number of partitions into different parts, no one of which has a zero component. Our object is to find an asymptotic formula for $p^{(5)}(m,n)$ for large m and n satisfying (1.1).

In what follows, $s=1,2,3$ or 4; any statement involving s is true for these four values of s. The letter s is frequently omitted, so that, for example, $p(m,n)$ is written for $p^{(s)}(m,n)$, a for $a^{(s)}$, and so on.

We write

$$a^{(1)}=a^{(2)}=\zeta(3)=\sum_{r=1}^{\infty} r^{-3}=1.20205690\cdots,$$

$$a^{(3)}=a^{(4)}=(3/4)\zeta(3),\quad b^{(1)}=-b^{(2)}=\pi^2/12,\quad b^{(3)}=-b^{(4)}=\pi^2/24,$$

and γ for Euler's constant, so that

$$\gamma=\lim_{r\to\infty}(1+1/2+1/3+\cdots+1/r-\log r)=0.5772157\cdots.$$

Again, for all complex z such that $\Re(z)>0$, we write

$$c^{(2)}(z)=(z+3+z^{-1})/24,\quad c^{(1)}(z)=c^{(2)}(z)-\tfrac{1}{2},\quad c^{(3)}(z)=c^{(4)}(z)=0,$$

and

$$I(z)=\int_0^\infty\{(u(e^{zu}-1)(e^u-1))^{-1}-z^{-1}u^{-3}+\tfrac{1}{2}(1+z^{-1})u^{-2}$$
$$-2c_2(z)(e^u-1)^{-1}\}du.$$

It is readily verified that this integral converges. Its evaluation is discussed in [5]. In particular, if $n=o(m)$, we have

$$I(n/m)=\alpha_{-1}m/n+\alpha_0+O(n^3/m^3), \tag{2.2}$$

where $\alpha_{-1}=(1-\gamma)/12-\zeta'(-1)=.20065317\cdots,$

$$\alpha_0=\tfrac{1}{4}\log(2\pi)-\tfrac{1}{4}\gamma=.31516535\cdots.$$

We write also

$$d^{(2)}(z)=c^{(2)}(z)(\log z+2\gamma)+I(z),$$

where $\log z$ has its principal value, and

$$d^{(1)}(z)=d^{(2)}(z)-\log 2\pi,\quad d^{(3)}=2c^{(1)}\log 2,\quad d^{(4)}=2c^{(2)}\log 2,$$

$$D(z)=d(z)-\log(2\pi a3^{\frac{1}{2}})-b^2(z-1+z^{-1})/3a.$$

A little calculation shows that $d^{(2)}(1/z) = d^{(2)}(z)$, and a similar result follows trivially for c, $d^{(1)}$, $d^{(3)}$, $d^{(4)}$ and D.

The numbers ϵ, ϵ_1, ϵ_2 are positive numbers, to be thought of as small. C is a positive number, not always the same at each occurrence, which may depend upon any of ϵ, ϵ_1, ϵ_2, s, h, k, but not on m, n, x, y, X, Y, θ, ϕ, ξ, η, u, t, z. The symbols $O(\ )$ and $o(\ )$ refer to the passage of m and n to infinity or of x, y, X, Y to zero. The constant implied in the $O(\ )$ notation is of type C and all statements are subject to the implied conditions "for $m > C$ and $n > C$" or "for $|x| < C$ and $|y| < C$," as may be appropriate.

We write

$$\mu = (amn^{-2})^{\frac{1}{3}}, \qquad \nu = (anm^{-2})^{\frac{1}{3}}, \tag{2.3}$$

so that, when (1.1) is satisfied, μ and ν are $o(1)$. We shall repeatedly make use of the relations

$$\mu^3\nu^3 = a^2/mn, \qquad \nu/\mu = n/m. \tag{2.4}$$

We write $T_1(t) = 0$ and

$$T_H(t) = a\sum_{h=3}^{2H-1} P_h t^{h-1} \qquad (H \geqq 2),$$

where $P_h^{(1)}$ and $P_h^{(2)}$ are polynomials in $\log t$ of degree $[\frac{1}{2}h]$, whose coefficients can be calculated, and $P_h^{(3)}$ and $P_h^{(4)}$ are numbers depending only on h and s. In particular,

$$P_h^{(2)} = (-1)^h P_h^{(1)}, \qquad P_h^{(4)} = (-1)^h P_h^{(3)}.$$

We show how to calculate P_h in § 7 and give a table of P_h for $h \leqq 7$ at the end of the paper.

Our object is to prove the following

THEOREM. *If m and n tend to infinity subject to the condition* (1.1), *we have $p(m,n) \sim e^{\sigma}$, that is*

$$\log p(m,n) = \sigma + o(1),$$

where

$$\sigma = 3(amn)^{\frac{1}{3}} + b(m+n)/(amn)^{\frac{1}{3}} + (1/3)\{2 - c(n/m)\}\log(a^2/mn)$$
$$+ D(n/m) + \nu^{-1}T_K(\mu) + \mu^{-1}T_{K'}(\nu)$$

and

$$K = [3/8\epsilon_1 + 3/2], \qquad K' = [3/2\epsilon_2 + 1/2].$$

Since σ is symmetrical in m and n, we can confine ourselves to the case in which

$$\tfrac{1}{2} + \epsilon_1 \leqq \log n / \log m \leqq 1, \tag{2.5}$$

i. e.,

$$m^{\frac{1}{2}+\epsilon_1} \leqq n \leqq m. \tag{2.6}$$

If we write $\epsilon_3 = 4\epsilon_1/3$, we have

$$\nu \leqq \mu \leqq \nu^{\epsilon_3}. \tag{2.7}$$

Hence $T_{K'}(\nu) = O(\nu^2 \log \nu) = o(\mu)$ and we may replace σ by

$$\sigma_1 = 3a/\mu\nu + b/\mu + b/\nu + \{2 - c(\nu/\mu)\} \log(\mu\nu) \\ + D(\nu/\mu) + \nu^{-1} T_K(\mu).$$

3. The integral for $p(m,n)$. We take X, Y small, positive numbers which we define more precisely later. For the present, we require only that

$$X \sim \nu, \qquad Y \sim \mu, \tag{3.1}$$

so that $X = O(Y)$ by (2.7).

We write $x = X + i\theta = X(1 + i\xi)$, $y = Y + i\phi = Y(1 + i\eta)$, where $-\pi \leqq \theta$, $\phi \leqq \pi$. We write also

$$\lambda^{(1)}(h,k) = \lambda^{(2)}(h,k) = (1 - e^{-hx-ky})^{-1},$$
$$\lambda^{(3)}(h,k) = \lambda^{(4)}(h,k) = 1 + e^{-hx-ky},$$

and

$$f^{(s)}(x,y) = \prod \lambda^{(s)}(h,k),$$

where, for $s = 2$ or 4, h and k each take all positive integral values, while, for $s = 1$ or 3, h and k each take all non-negative integral values, except $h = k = 0$. We see at once that

$$f^{(3)}(x,y) = f^{(1)}(x,y)/f^{(1)}(2x,2y), \quad f^{(4)}(x,y) = f^{(2)}(x,y)/f^{(2)}(2x,2y). \tag{3.2}$$

If we put $p(0,0) = 1$, we verify from the definitions that

$$f(x,y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} p(m,n) e^{-mx-ny}. \tag{3.3}$$

Hence

$$\begin{aligned} p(m,n) &= (1/4\pi^2) \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} f(x,y) e^{nx+ny} \, d\theta d\phi \\ &= (XY/4\pi^2) \int_{-\pi/Y}^{\pi/Y} \int_{-\pi/X}^{\pi/X} e^{F(x,y)} \, d\xi d\eta, \end{aligned} \tag{3.4}$$

where

$$F(x,y) = mx + ny + \log f(x,y).$$

We choose ϵ a fixed positive number small enough to ensure that

$$(3.5) \qquad 22\epsilon < 1, \qquad 12\epsilon < \epsilon_3$$

and that

$$(3.6) \qquad [\tfrac{1}{2}(1+6\epsilon)(1+1/\epsilon_3)] = [\tfrac{1}{2}(1+1/\epsilon_3)] = [3/8\epsilon_1 + \tfrac{1}{2}] = K - 1.$$

We write

$$\zeta = (\mu\nu)^{\frac{1}{2}-3\epsilon} = C(mn)^{\epsilon-(1/6)}, \qquad U = \zeta(XY)^{-\frac{1}{2}} \sim C(mn)^{\epsilon}.$$

By a similar argument to that used to prove Lemma 1 of [4], we can prove

LEMMA 1. *If* $\tfrac{1}{2}\zeta \leqq |\xi| \leqq \pi/X$ *or if* $\tfrac{1}{2}\zeta \leqq |\eta| \leqq \pi/Y$, *then*

$$|F(x,y)| \leqq F(X,Y) - CU^2.$$

We shall prove later

LEMMA 2. *We can choose* X *and* Y *to satisfy* (3.1) *and such that*

$$F(x,y) - F(X,Y) = -(a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1),$$

whenever

$$(3.7) \qquad |\xi| + |\eta| \leqq \zeta.$$

Using these two lemmas, we have from (3.4) that

$$p(m,n) \sim (XYe^{F(X,Y)}/4\pi^2)\{\iint_{|\xi|+|\eta|\leqq\zeta} \exp\{-(a/XY)(\xi^2+\xi\eta+\eta^2)\}\,d\xi d\eta + O(e^{-CU^2}/XY)\}.$$

If we put

$$\xi = (XY)^{\frac{1}{2}}(u+v), \qquad \eta = (XY)^{\frac{1}{2}}(u-v),$$

we have

$$\iint_{|\xi|+|\eta|\leqq\zeta} \exp\{-(a/XY)(\xi^2+\xi\eta+\eta^2)\}\,d\xi d\eta$$

$$= 2XY \int_{-U}^{U}\int_{-U}^{U} \exp(-3au^2 - av^2)\,du dv$$

$$\sim 2XY \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp(-3au^2 - av^2)\,du dv = 2\pi XY/3^{\frac{1}{2}}a.$$

Hence

$$p(m,n) = X^2Y^2e^{F(X,Y)}(3^{\frac{1}{2}}\cdot 2\pi a)^{-1}\{1 + o(1) + O(X^{-2}Y^{-2}e^{-CU^2})\} \sim e^{\sigma_2},$$

where

$$\sigma_2 = F(X,Y) + 2\log(\mu\nu) - \log(3^{\frac{1}{2}}\cdot 2\pi a).$$

It remains to prove Lemma 2 and to show that

$$\sigma_2 = \sigma_1 + o(1),$$

that is, that

$$(3.8) \qquad F(X,Y) = 3a/\mu\nu + b/\mu + b/\nu - c(\nu/\mu)\log(\mu\nu) + D(\nu/\mu) + \log(3^{\frac{1}{2}}\cdot 2\pi a) + \nu^{-1}T_K(\mu) + o(1).$$

4. **Further results.** We use B_k for the k-th Bernoulli number, where

$$u/(e^u-1) = 1 - \tfrac{1}{2}u + \sum_{k=1}^{\infty}(-1)^{k-1}B_k u^{2k}/(2k)! \qquad (|u| < 2\pi),$$

and write

$$\gamma_k^{(1)} = \gamma_k^{(2)} = -B_kB_{k+1}/2ka^{(1)}(2k+2)!,$$

$$\gamma_k^{(3)} = \gamma_k^{(4)} = B_kB_{k+1}(2^{2k}-1)/2ka^{(3)}(2k+2)!, \quad (k \geqq 1)$$

$$S_1(x) = 0, \qquad S_H(x) = \sum_{h=1}^{H-1}\gamma_h x^{2h+1} \qquad (H \geqq 2).$$

Henceforth we suppose that (3.7) is satisfied. Then, for any $H \geqq 1$, we can deduce from Theorem 1 of [6] that

$$F(x,y) = mx + ny + a/xy + b/x + b/y - aS_H(x)/y - aS_H(y)/x - c(x/y)\log(xy) + d(x/y) + O(x) + O(y) + O(x^{2H+1}y^{-1}) + O(y^{2H+1}x^{-1}).$$

By (3.1) and (2.7), we have

$$x \sim X \sim \nu, \qquad y \sim Y \sim \mu, \qquad x = O(y) = o(1),$$

and so

$$S_H(x) = O(x^3) = O(y^3) = o(y), \quad x^{2H+1}y^{-1} = O(x^3y^{-1}) = o(1).$$

Hence

$$(4.1) \qquad F(x,y) = mx + ny + a/xy + b/x + b/y - aS_H(y)/x - c(x/y)\log(xy) + d(x/y) + O(y^{2H+1}/x) + o(1).$$

We now introduce the linear operator Ω defined by

$$\Omega g(x,y) = g(x,y) - g(X,Y) - i\xi X(\partial/\partial X)g(X,Y) - i\eta Y(\partial/\partial Y)g(X,Y)$$

where g is any function of the two variables x and y with continuous first derivatives. Trivial calculations show that

$$\Omega(1/xy) = -(\xi^2 + \xi\eta + \eta^2)/XY + O(\zeta^3/XY),$$

$$\Omega(1/x) = O(\zeta^2/X), \qquad \Omega(1/y) = 0(\zeta^2/Y), \qquad \Omega(x) = \Omega(y) = 0.$$

Now

$$\zeta^3/(XY) = O\{(\mu\nu)^{\frac{1}{2}-9\epsilon}\} = o(1),$$

$$\zeta^2/Y = O(\zeta^2/X) = O(\mu^{1-6\epsilon}\nu^{-6\epsilon}) = O(\nu^{\epsilon_3-6\epsilon\epsilon_3-6\epsilon}) = o(1),$$

since $12\epsilon < \epsilon_3$ by (3.5). Again,

$$\Omega(y^{2h+1}/x) = O(\zeta^2 Y^{2h+1}/X) = o(\zeta^2/X) = o(1) \tag{4.2}$$

when $h \geqq 0$, and

$$\Omega(y\log y/x) = O(\zeta^2 Y\log Y/X) = o(\zeta^2/X) = o(1). \tag{4.3}$$

Hence

$$\Omega(1/xy) = -(\xi^2 + \xi\eta + \eta^2)/XY + o(1);$$

and

$$\Omega(1/x), \Omega(1/y), \Omega(x), \Omega(y), \Omega(y^{2h+1}/x), \Omega(x^{-1}y\log y)$$

are all $o(1)$.

We now consider separately the case in which $m^{5/6} \leqq n \leqq m$ and that in which $m^{\frac{1}{2}+\epsilon_1} \leqq n \leqq m^{5/6}$.

5. The case $m^{5/6} \leqq n \leqq m$. In this case we have

$$\log\nu \leqq \log\mu \leqq 4\log\nu/7 + C$$

and so

$$2\log\mu - \log\nu \leqq C + \log\nu/7,$$

$$\begin{aligned}2\log\zeta - \log\nu &= (1-6\epsilon)\log\mu - 6\epsilon\log\nu \\ &\leqq C + (4/7 - 66\epsilon/7)\log\nu < C + \log\nu/7,\end{aligned}$$

since $22\epsilon < 1$ by (3.5). Hence

$$\mu^2/\nu = O(\nu^{1/7}), \qquad \zeta^2/\nu = O(\nu^{1/7}), \qquad \mu\zeta/\nu = O(\nu^{1/7}). \tag{5.1}$$

From the first of these it follows that $y^3/x \sim \mu^3/\nu = o(1)$. Hence, if we put $H = 1$ in (4.1), we have

$$(5.2) \qquad F(x,y) = F_1(x,y) + F_2(x,y) + o(1),$$

where

$$F_1(x,y) = mx + ny + a/xy + b/x + b/y,$$
$$F_2(x,y) = d(x/y) - c(x/y)\log(xy).$$

It follows from the results of the last section that

$$\Omega F_1(x,y) = -(a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1)$$

and so that

$$(5.3) \quad F_1(x,y) - F_1(X,Y)$$
$$= i\xi X\partial F_1/\partial X + i\eta Y\partial F_1/\partial Y - (a/XY)(\xi^2 + \xi\eta + \eta^2) + o(1).$$

We now choose

$$(5.4) \qquad X = \nu\{1 + ba^{-1}(2\mu - \nu)/3\}, \qquad Y = \mu\{1 + ba^{-1}(2\nu - \mu)/3\}.$$

We have

$$X(\partial/\partial X)F_1(X,Y) = mX - a/XY - b/X = (mX^2Y - a - bY)/XY.$$

Since $\nu = O(\mu)$,

$$mX^2Y = m\nu^2\mu\{1 + ba^{-1}(2\mu - \nu)/3\}^2\{1 + ba^{-1}(2\nu - \mu)/3\}$$
$$= a + b\mu + O(\mu^2) = a + bY + O(\mu^2)$$

and

$$(5.5) \qquad \xi X\partial F_1/\partial X = O(\zeta\mu^2/XY) = O(\zeta\mu/\nu) = o(1).$$

A similar calculation shows that

$$(5.6) \qquad \eta Y(\partial F_1/\partial Y) = o(1).$$

and so (5.3) becomes

$$(5.7) \qquad F_1(x,y) - F_1(X,Y) = -a(\xi^2 + \xi\eta + \eta^2)(XY)^{-1} + o(1).$$

The choice of X, Y in (5.4) is, of course, designed to ensure the truth of (5.5) and (5.6), i.e., to take X, Y not at the "saddle-point" but sufficiently near to it.

By (5.4),

$$(5.8)\qquad x/y = X(1+i\xi)/Y(1+i\eta) = (X/Y)\{1+O(\zeta)\}$$
$$= (\nu/\mu)\{1+O(\mu)+O(\zeta)\} = (\nu/\mu)+O(\nu)+O(\zeta\nu/\mu).$$

Again,

$$|F_2(x,y)-F_2(\nu,\mu)| \leqq C\mu^2/\nu^2\,|\log(\mu\nu)|\,|x/y-\nu/\mu| + |I(x/y)-I(\nu/\mu)|$$
$$+o(1).$$

We can show, by the methods of [5], that

$$|I(x/y)-I(\nu/\mu)| \leqq C|x/y-\nu/\mu|\,\mu^2/\nu^2,$$

provided that this is $o(1)$. Now

$$(\mu^2/\nu^2)\,|x/y-\nu/\mu| = O(\mu^2/\nu)+O(\zeta\mu/\nu) = O(\nu^C)$$

by (5.8) and (5.1). Again, $\log(\mu\nu) = O(\log\nu)$ and so

$$(5.9)\qquad F_2(x,y)-F_2(\nu,\mu) = o(1).$$

In the special case $x=X$, $y=Y$, this is

$$(5.10)\qquad F_2(X,Y)-F_2(\nu,\mu) = o(1).$$

From (5.2), (5.7), (5.9) and (5.10), we have Lemma 2 for this case. Again, in this case,

$$T_K(\mu) = O(\mu^2\log\mu) = o(\nu)$$

and so, to prove (3.8), it is enough to show that

$$F_1(X,Y)+F_2(X,Y) = 3a/\mu\nu+b/\mu+b/\nu-c(\nu/\mu)\log(\mu\nu)$$
$$+D(\nu/\mu)+\log(3^{1/2}\cdot 2\pi a)+o(1),$$

that is, in virtue of (5.10) and the definitions of $D(z)$ and $F_1(X,Y)$, that

$$mX+nY+a/XY+b/X+b/Y$$
$$= 3a/\mu\nu+b/\mu+b/\nu-b^2(\nu/\mu-1+\mu/\nu)/3a+o(1).$$

This follows from (5.4) and the first part of (5.1) with a little calculation.

6. The case $m^{1/2+\epsilon_1} \leqq n \leqq m^{5/6}$. In this case we have

$$x/y \sim X/Y \sim \nu/\mu = n/m = o(1), \qquad x\log y/y = o(1),$$
$$\log y = \log\mu+o(1).$$

Now, by [5], if $|\arg z| < \frac{1}{2}\pi - C$,

$$I(z) = \{(1-\gamma)/12 - \zeta'(-1)\}/z - (\gamma - \log 2\pi)/4 + O(z^3).$$

Hence, if we write $\alpha = b/3a$,

$$\gamma_0 = (12\zeta'(-1) - 1)/12a, \qquad \beta = -1/12a \quad (s = 1, 2),$$

$$\gamma_0 = -\log 2/12a, \quad \beta = 0 \quad (s = 3, 4),$$

$$A^{(1)} = [\log(\mu\nu^2/8\pi^3)]/4, \qquad A^{(2)} = [\log({}^2\pi/\mu)]/4,$$

$$A^{(3)} = -(3\log 2)/4, \qquad A^{(4)} = (\log 2)/4,$$

we have

$$(6.1) \qquad d(\nu/\mu) - c(\nu/\mu)\log(\mu\nu) = A + a\mu\nu^{-1}(\beta\log\mu - \gamma_0) + o(1)$$

and

$$(6.2) \qquad d(x/y) - c(x/y)\log(xy) = A + ayx^{-1}(\beta\log y - \gamma_0) + o(1).$$

Again, by (2.7) and the definitions of K,

$$y^{2K+1}/x \sim \mu^{2K+1}/\nu = O(\nu^{(2K+1)\epsilon_3 - 1}) = o(1).$$

Hence, if we take $H = K$ in (4.1), we have

$$(6.3) \qquad F(x, y) = F_4(x, y) + A + by^{-1} + o(1),$$

where

$$F_4(x, y) = mx + ny + a(xy)^{-1}\chi_K(y),$$

$$\chi_H(y) = 1 + 3\alpha y + y^2(\beta\log y - \gamma_0) - yS_H(y).$$

Now

$$b/y - b/Y = -i\eta/Y(1 + i\eta) = O(\zeta/\mu) = O(\mu^{-\frac{1}{2}-3\epsilon}\nu^{\frac{1}{2}-3\epsilon})$$
$$= O(n^{\frac{1}{2}+\epsilon}m^{-\frac{1}{2}+\epsilon}) = O(m^{(22\epsilon-1)/12}) = o(1),$$

since $n \leqq m^{5/6}$ and $22\epsilon < 1$. Hence

$$F(x, y) - F(X, Y) = F_4(x, y) - F_4(X, Y) + o(1).$$

Now the results of § 4 show that

$$\Omega F_4(x, y) = -a(\xi^2 + \xi\eta + \eta^2)(XY)^{-1} + o(1)$$

and so, to prove Lemma 2, we have only to choose X and Y so that

$$\xi X(\partial F_4/\partial X) = o(1), \qquad \eta Y(\partial F_4/\partial Y) = o(1),$$

that is, so that

$$(6.4)\qquad mX^2Y - a\chi_K(Y) = o(XY/\zeta) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}$$

and

$$(6.5)\qquad nXY^2 - a\omega_K(Y) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\},$$

where

$$\omega_H(Y) = \chi_H(Y) - Y\chi'_H(Y) = 1 - Y^2(\beta\log Y + \beta - \gamma_0) + Y^2S'_H(Y).$$

We write $\delta = \beta\log\mu - \gamma_0$, so that $C < \delta/|\log\mu| < C$ when $s = 1$ or 2, and $\delta = -\gamma_0 = C$ when $s = 3$ or 4.

In the next section we shall prove

LEMMA 3. *For every positive integer h, there exist two polynomials Q_h, R_h of degree $[\frac{1}{2}h]$ in δ whose coefficients depend only on h and s and which have the following property. If*

$$(6.6)\qquad X_H = 1 + \sum_{h=1}^{H-1} R_h\mu^h, \qquad Y_H = 1 + \sum_{h=1}^{H-1} Q_h\mu^h,$$

then

$$(6.7)\qquad X_H{}^2Y_H = \chi_H(\mu Y_H) + O(\mu^H\delta^{[\frac{1}{2}H]}),$$

$$(6.8)\qquad X_HY_H{}^2 = \omega_H(\mu Y_H) + O(\mu^H\delta^{[\frac{1}{2}H]}).$$

By (3.6)

$$K = [(\tfrac{1}{2} + 3\epsilon)(1 + 1/\epsilon_3)] + 1 > (\tfrac{1}{2} + 3\epsilon)(1 + 1/\epsilon_3) + C$$

and so

$$\epsilon_3(K - \tfrac{1}{2} - 3\epsilon) > \tfrac{1}{2} + 3\epsilon + C.$$

Hence, by (2.7),

$$\mu^{K-\frac{1}{2}-3\epsilon} \leqq \nu^{\epsilon_3(K-\frac{1}{2}-3\epsilon)} < \nu^{\frac{1}{2}+3\epsilon+C}$$

and so

$$(6.9)\qquad \mu^K\delta^{[\frac{1}{2}K]} < (\mu\nu)^{\frac{1}{2}+3\epsilon}\nu^C = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}.$$

We now choose $X = \nu X_H$, $Y = \mu Y_H$, so that $X \sim \nu$ and $Y \sim \mu$ as we have supposed. We remark that $m\mu\nu^2 = n\nu\mu^2 = a$. Then, by (6.9) and Lemma 3 with $H = K$, we have

$$m/X^2Y - a\chi_K(Y) = aX_K{}^2Y_K - a\chi_K(\mu Y_K) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}$$

and

$$n/XY^2 - a\omega_K(Y) = aX_KY_K{}^2 - a\omega_K(\mu Y_K) = o\{(\mu\nu)^{\frac{1}{2}+3\epsilon}\}.$$

Hence (6.4) and (6.5) are satisfied and the proof of Lemma 2 is complete.

With these values of X and Y, we have

$$\begin{aligned} F(X,Y) &= F_4(X,Y) + A + (b/Y) + o(1) \\ &= mX + nY + a\chi_K(Y)(XY)^{-1} + A + b/Y + o(1) \\ &= a\Lambda_K/\mu\nu + A + b/\mu - bQ_1 + o(1), \end{aligned}$$

where

(6.10) $$\begin{aligned} \Lambda_H &= X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H \\ &= 3 + \sum_{h=1}^{2H-1} P_h \mu^h + O(\mu^{2H}\delta^H) \end{aligned}$$

and P_h is a polynomial of degree $[\frac{1}{2}h]$ in δ. In the next section we shall see how to calculate

$$Q_1 = -\alpha, \qquad P_1 = 3\alpha, \qquad P_2 = \delta - 3\alpha^2.$$

Hence

$$\begin{aligned} F(X,Y) = 3a/\mu\nu + b/\mu + b/\nu + A + b\alpha + a\mu(\delta - 3\alpha^2)/\nu + \sum_{h=3}^{2K-1} aP_h\mu^{h-1}/\nu \\ + O(\mu^{2K-1}\nu^{-1}\delta^K) + o(1), \end{aligned}$$

and (3.8) follows from this and (6.1) and (6.9).

7. Proof of Lemma 3 and calculation of P_h. From (6.7) and (6.8), we obtain

(7.1) $$Y_H^3\chi_H(\mu Y_H) = \{\omega(\mu Y_H)\}^2 + O(\mu^H \delta^{[\frac{1}{2}H]}),$$

whence

(7.2) $$Y_H = 1 + \sum_{h=1}^{H-1} q_h \mu^h Y_H^h + O(\mu^H \delta^{[\frac{1}{2}H]}),$$

where q_h is a polynomial of degree $[\frac{1}{2}h]$ at most in $\beta \log(\mu Y_H) - \gamma_0 = \delta + \beta \log Y_H$. With sufficient labour, we can solve (7.2) by successive approximations to Y_H of the form

$$Y_H = 1 + Q_1\mu + O(\mu^2\delta), \qquad Y_H = 1 + Q_1\mu + Q_2\mu^2 + O(\mu^3\delta), \ldots$$

and eventually we have

$$Y_H = 1 + \sum_{h=1}^{H-1} Q_h \mu^h.$$

From this and (6.8), we deduce

$$X_H = Y_H^{-2}\omega(\mu Y_H) + O(\mu^H \delta^{[\frac{1}{2}H]}) = 1 + \sum_{h=1}^{H-1} R_h \mu^h.$$

Retracing our steps we see that these X_H and Y_H must satisfy (6.7) and (6.8).

We could, of course, add any terms in μ^H and higher powers to X_H and Y_H without affecting the truth of (6.7) and (6.8). Again

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)(X_H Y_H)^{-1}$$

and so

$$\partial\Lambda_H/\partial X_H = 1 - \chi_H(\mu Y_H)/X_H^2 Y_H = O(\mu^H \delta^{[\frac{1}{2}H]}) \tag{7.3}$$

by (6.7), and similarly

$$\partial\Lambda_H/\partial Y_H = 1 - \omega_H(\mu Y_H)/X_H Y_H^2 = O(\mu^H \delta^{[\frac{1}{2}H]}) \tag{7.4}$$

by (6.8). Hence a change in X_H or Y_H of order $O(\mu^H\delta^{[\frac{1}{2}H]})$ will produce a change of not more than $O(\mu^{2H}\delta^H)$ in Λ_H. Now $X_{H+1} - X_H$ and $Y_{H+1} - Y_H$ are $O(\mu^H\delta^{[\frac{1}{2}H]})$ and $\chi_{H+1}(\mu Y_{H+1}) - \chi_H(\mu Y_{H+1}) = O(\mu^{2H})$. Hence

$$\Lambda_{H+1} - \Lambda_H = O(\mu^{2H}\delta^H)$$

and so in (6.10) the polynomials P_h are independent of H.

We have shown above that Q_h, R_h, P_h exist and can be calculated, but the method of calculation is plainly very laborious. We can, however, shorten the calculations considerably by the following considerations. From (6.7), we have

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H = 2X_H + Y_H + O(\mu^H\delta^{[\frac{1}{2}H]}) \tag{7.5}$$

and so, if we equate coefficients of μ^h, we have

$$2R_h + Q_h = P_h. \tag{7.6}$$

Again,

$$\Lambda_H = X_H + Y_H + \chi_H(\mu Y_H)/X_H Y_H = 3 + \sum_{h=1}^{2H-1} P_h\mu^h + \sum_{h=2H}^{\infty} L_h\mu^h,$$

where L_h is a polynomial in δ of degree $[\frac{1}{2}h]$. This infinite series and its derived series are uniformly and absolutely convergent when $0 < \mu < C$ for some C. Hence

$$\mu(d\Lambda_H/d\mu) = \sum_{h=1}^{2H-1}(hP_h + \beta(dP_h/d\delta))\mu^h + O(\mu^{2H}\delta^H).$$

Now

$$\begin{aligned}\mu(d\Lambda_H/d\mu) &= \mu(\partial\Lambda_H/\partial X_H)(dX_H/d\mu)\\ &\qquad + \mu(\partial\Lambda_H/\partial Y_H)(dY_H/d\mu) + \mu\chi'_H(\mu Y_H)/X_H.\end{aligned}$$

The first two terms on the right are $O(\mu^{H+1}\delta^{[\frac{1}{2}H]})$ by (7.3) and (7.4). Again

$$\chi'_H(\mu Y_H)\mu Y_H = \chi_H(\mu Y_H) - \omega_H(\mu Y_H) = X_H{}^2 Y_H - X_H Y_H{}^2 + O(\mu^H \delta^{[\frac{1}{2}H]})$$

by (6.7) and (6.8). Hence

$$\mu(d\Lambda_H/d\mu) = X_H - Y_H + O(\mu^H\delta^{[\frac{1}{2}H]}).$$

Thus, if we equate "coefficients" of μ^h, we have

$$R_h - Q_h = hP_h + \beta(dP_h/d\delta). \tag{7.7}$$

From (7.6) and (7.7), we have at once

$$\begin{aligned} Q_h &= -(2h-1)P_h/3 - (2\beta/3)(dP_h/d\delta), \\ R_h &= (h+1)P_h/3 + (\beta/3)(dP_h/d\delta). \end{aligned} \tag{7.8}$$

Our method of calculation is now fairly simple. Given Q_h and R_h for $1 \leqq h \leqq H-1$, we use (6.10) to calculate P_h for $H \leqq h \leqq 2H-1$ and (7.8) to calculate Q_h and R_h for $H \leqq h \leqq 2h-1$. We then repeat the process with $2H$ for H. We start with $H=1$, $X_1 = Y_1 = 1$ and can thus calculate P_h for any h. We thus avoid having to solve (7.1) or (7.2), which would be troublesome. The only stage of each cycle which is at all elaborate is the use of (6.10). Using (7.6) in (6.10), we have

$$\chi_H(\mu Y_H)/X_H Y_H = 1 + \sum_{h=1}^{H-1} R_h\mu^h + \sum_{h=H}^{2H-1} P_h\mu^h + O(\mu^{2H}\delta^H).$$

Now

$$\begin{aligned} \chi_H(\mu Y_H)/Y_H &= Y_H{}^{-1} + 3\alpha\mu + \delta\mu^2 Y_H - \sum_{k=1}^{H-2}\gamma_k\mu^{2k+2}Y_H{}^{2k+1} + O(\mu^{2H}) \\ &= 1 + \sum_{h=1}^{2H-1} M_h\mu^h + O(\mu^{2H}\delta^H), \end{aligned}$$

where we can calculate the M_h. Finally,

$$\begin{aligned} 1 + \sum_{h=1}^{2H-1} M_h\mu^h = {} & (1 + \sum_{h=1}^{H-1} R_h\mu^h)(1 + \sum_{h=1}^{H-1} R_h\mu^h + \sum_{h=H}^{2H-1} P_h\mu^h) \\ & + O(\mu^{2H}\delta^H) \end{aligned}$$

and we calculate $P_H, \cdots, P_{2H-1}$ from

$$P_H = M_H - \sum_{h=1}^{H-1} R_h R_{H-h},$$

$$P_{H+1} = M_{H+1} - R_1 P_H - \sum_{h=2}^{H-1} R_h R_{H+1-h},$$

and so on in succession.

If we replace α by $-\alpha$, μ by $-\mu$ but leave δ unchanged (i.e., leave $\log\mu$ unchanged), the sums $\chi_H(\mu Y_H)$ and $\omega_H(\mu Y_H)$ are the same functions of α, μ, δ, Y_H as before. Hence the equation (7.2) is unaltered and so Y_H is unchanged, and so, also, X_H and Λ_H. Hence P_h is an odd or even function of α according as h is odd or even. Since $\alpha^{(2)}=-\alpha^{(1)}$ and $\alpha^{(4)}=-\alpha^{(3)}$, we have

$$P_h^{(2)}=(-1)^hP_h^{(1)}, \qquad P_h^{(4)}=(-1)^hP_h^{(3)}.$$

This remark exactly halves our labour.

We conclude by giving P_h for $h\leqq 7$, first as a polynomial in δ with coefficients in terms of α, β, γ_1, γ_2 and secondly with numerical values.

We have

$$P_0=3,\ P_1=3\alpha,\ P_2=\delta-3\alpha^2,\ P_3=-3\alpha\delta-\alpha\beta+7\alpha^3$$

$$P_4=-\delta^2+\delta(12\alpha^2-\beta)-\beta^2/3+11\beta\alpha^2/2-22\alpha^4-\gamma_1,$$

$$P_5=8\alpha\delta^2+\delta\alpha(9\beta-54\alpha^2)+3\beta^2\alpha-57\beta\alpha^3/2+81\alpha^5+5\gamma_1\alpha,$$

$$\begin{aligned}P_6=2\delta^3&+\delta^2(23\beta/6-55\alpha^2)+\delta(8\beta^2/3-66\beta\alpha^2+260\alpha^4+4\gamma_1)\\&+17\beta^3/27-133\beta^2\alpha^2/6+1787\beta\alpha^4/12-988\alpha^6/3\\&+7\beta\gamma_1/3-25\gamma_1\alpha^2-\gamma_2,\end{aligned}$$

$$\begin{aligned}P_7=-27\alpha\delta^3&+\delta^2\alpha(1078\alpha^2/3-319\beta/6)\\&+\delta\alpha(-112\beta^2/3+1351\beta\alpha^2/3-1309\alpha^4-38\gamma_1)\\&-242\beta^3\alpha/27+2753\beta^2\alpha^3/18-47477\beta\alpha^5/60+4301\alpha^7/3\\&-71\beta\gamma_1\alpha/3+385\gamma_1\alpha^3/3+7\gamma_2\alpha.\end{aligned}$$

If we write

$$P_h^{(1)}=\sum_{k=0}^{[\frac{1}{2}h]}\rho_{hk}(\log\mu)^k,$$

we have the following table for ρ_{hk}.

$h\diagdown k$	0	1	2	3
1	.68421639			
2	.05088999	—.06932561		
3	—.04273573	.04743372		
4	.01982883	—.01938670	—.00480604	
5	—.00728059	.00192568	.00876899	
6	.00133717	.00576762	—.00905955	—.00066636
7	.00097131	—.00713373	.00615476	.00205172

For $s = 3$, we find that

$P_1 = .45614426$

$P_2 = -.00528539$

$P_3 = -.00461938$

$P_4 = .00152613$

$P_5 = -.00029313$

$P_6 = .00001197$

$P_7 = .00001931$

The following short table of values of $I(n/m)$ was caluculated from the results of [5] by Mr. M. M. Robertson.

$I(0.1) = 2.321694$

$I(0.2) = 1.313405$

$I(0.3) = 0.983921$

$I(0.4) = 0.816592$

$I(0.5) = 0.716076$

$I(0.6) = 0.648918$

$I(0.7) = 0.600774$

$I(0.8) = 0.564468$

$I(0.9) = 0.536012$

$I(1.0) = 0.513011$

UNIVERSITY OF ABERDEEN, SCOTLAND.

REFERENCES.

[1] F. C. Auluck, *Proceedings of the Cambridge Philosophical Society*, vol. 49 (1953), pp. 72-83.

[2] G. Meinardus, *Mathematische Annalen*, vol. 132 (1956), pp. 333-346.

[3] V. S. Nanda, *Proceedings of the Cambridge Philosophical Society*, vol. 53 (1957), pp. 273-277.

[4] E. M. Wright, *Proceedings of the London Mathematical Society*, ser. (3), vol. 7 (1957), pp. 150-160.

[5] ———, *ibid.*, ser. (3), vol. 8 (1958), pp. 312-320.

[6] ———, *Quarterly Journal of Mathematics* (in press).

PRINCIPAL HOMOGENEOUS SPACES OVER ABELIAN VARIETIES.*

By SERGE LANG and JOHN TATE.[1]

Let A be a commutative group variety defined over a field k. If K/k is a Galois extension, the group A_K of points of A rational over K is a module for the Galois group $G(K/k)$, and we denote the associated cohomology groups simply by $H^r(K/k, A)$ or by $H^r(k, A)$ in case K is the separable closure of k. In case K/k is infinite, we mean of course the cohomology groups constructed with cochains of finite type, i.e. coming by inflation from finite extensions.

In § 1, we have carried over to the infinite case the basic propositions of Galois cohomolgy which are familiar in the finite case [2]. This generalization is essentially trivial, but it furnishes a good review for the non-expert, it fixes our notation, and mainly, it is urgently called for when one studies algebraic groups for the following reason: If $A \rightarrow B \rightarrow C$ is an exact sequence of (separable) homomorphisms defined over k, then $A_K \rightarrow B_K \rightarrow C_K$ is not necessarily exact but *is* exact if K is the (separable) algebraic closure of k. Actually, in the remainder of the paper, we require the cohomological results only for dimension 1, and most of our applications are based on the special "Kummer sequence" discussed at the end of § 1.

In § 2 we discuss systematically the representation of principal homogeneous spaces for A over k by elements of the 1-dimensional cohomology group (a set if A is non-commutative) $H^1(k, A)$. One establishes an injection of the classes of k-isomorphic spaces into $H^1(k, A)$, and as Serre has remarked, using Weil's theorems concerning the field of definition of a variety, one sees immediately that one actually gets a bijection. Since this representation has been carried out in special cases by F. Chatelet, we call $H^1(k, A)$ the Chatelet group.

Although the rest of the paper is essentially independent of the principal homogeneous space interpretation, it is mainly this interpretation and the consequent relation of the cohomology to diophantine problems which motivates our study of $H^1(k, A)$. For example, as Chatelet has shown, an

---

* Received January 7, 1958.

[1] Fulbright and Sloan Fellows respectively.

elliptic curve Γ is a homogeneous space over its Jacobian A, and the question whether Γ has a rational point in an extension field K is the same as whether its cohomology class $\alpha(\Gamma) \in H^1(k, A)$ is split by K.

The essential content of this paper is contained in the theorems of the last two sections, which concern the structure of $H^1(k, A)$ when A is an abelian variety.

We first consider the case where k is a local field. After recalling in § 3 some basic facts concerning reduction mod $\mathfrak{p}$, we treat in § 4 the case when A has a non-degenerate reduction. We show (Theorem 1) how the study of elements of order prime to p in $H^1(k, A)$ can be reduced to a study of the reduced variety. There results (Theorem 2) a complete description of the part of $H^1(k, A)$ prime to p when k is a $\mathfrak{p}$-adic number field. In particular, it is a finite group.

In § 5, we deal with global fields, essentially number fields, function fields over algebraically closed fields, or fields of finite type, and obtain various qualitative results. Theorem 3 gives a new variant of the proof that A_k/mA_k is finite. (For another variant, cf. Roquette [10].) From it, we deduce the finiteness of $H^r(K/k, A)$ for finite K/k and all $r > 0$, in Theorem 4. We then consider the subgroup of $H^1(k, A)$ consisting of those elements which split at all primes. Although it is known that this group is not necessarily trivial, we can show that for each integer m (prime to the characteristic of k), its subgroup of elements of period m is finite.

Theorems 6 and 7, which are independent of the preceding five, show on the other hand that $H^1(k, A)$ is large, in different senses. From Theorem 7, it is a corollary that given any positive integer m one can construct a function field in one variable of genus 1, over a suitable algebraic number field k, the degrees of whose divisors rational over k are exactly the multiples of m. One still does not have such examples when $k = \boldsymbol{Q}$ is the field of rational numbers.

1. **Galois cohomology.**

Let k be a field and Ω an algebraically closed field containing k. In Galois cohomology, one deals with a functor A which attaches to each field K between k and Ω a group $A(K)$ and to each k-isomorphism $\phi: K \rightarrow K^{\phi}$, an isomorphism $A(\phi): A(K) \rightarrow A(K^{\phi})$. The functor is subjected to three axioms:

(A1) For each K we have $A(K) = \bigcup A(F)$, the union being taken over all finitely generated subextensions F/k of K/k.

Notice that (A1) implies that all of our groups $A(K)$ are subgroups of one big group, namely $A(\Omega)$, and that we have $A(K) \subset A(L)$ whenever $K \subset L$.

(A2) If ψ prolongs ϕ, then $A(\psi)$ prolongs $A(\phi)$. If ψ and ϕ can be composed, then $A(\psi \circ \phi) = A(\psi) \circ A(\phi)$. A(identity) = identity.

From (A2) it follows that any group of k-automorphisms of a field L operates on $A(L)$.

(A3) If L/K is a Galois extension, then $A(K)$ is the set of fixed points for the operation of the Galois group on $A(L)$.

In most of our applications, A will be (the functor derived from) an algebraic group defined over k, for which $A(K) = A_K$ is the group of points of A which are rational over K, i.e. whose coordinates lie in K, and $A(\phi)$ is the map obtained by applying ϕ to the coordinates.

From now on in this section, we assume that our functor A is commutative, that is, each $A(K)$ is a commutative group. Let K/k be a (possibly infinite) Galois extension. Then $A(K)$ is a module for the Galois group $G(K/k)$, and we can consider the standard r-cochains $a = a(\sigma_1, \cdots, \sigma_r)$ of $G(K/k)$ with values in $A(K)$. We shall say that such a cochain is of *finite type* if there exists a finite sub-extension F such that $a(\sigma_1, \cdots, \sigma_r)$ depends only on the effects of the automorphisms σ_i on F. The cochains of finite type, which are the only ones arising from the usual algebraic processes, form a subcomplex of the standard cochain complex. We shall denote this subcomplex simply by $C(K/k, A)$ and its cohomology groups by $H^r(K/k, A)$. These latter are what we mean by Galois cohomology groups. Of course, if K/k is a finite extension then every cochain is of finite type, and we have achieved nothing but a simplification of notation: $H^r(K/k, A) = H^r(G(K/k), A(K))$. Also, even for infinite K, we have $H^0(K/k, A) = H^0(G(K/k), A(K))$ and this group is just $A(k)$ because of (A3). However, for $r > 0$ and K/k infinite, our groups may differ from the usual ones. For example, if $A(k) = A(K)$, that is, if $G(K/k)$ operates trivially on $A(K)$, then $H^1(K/k, A)$ is the group of continuous homomorphisms of $G(K/k)$ (Krull topology) into $A(K)$ (discrete topology), whereas $H^1(G(K/k), A(K))$ is the group of all homomorphisms.

Let K'/k' be another Galois extension, such that $K' \supset K$ and $k' \supset k$. Then each cochain $a \in C(K/k, A)$ determines a cochain $a' \in C(K'/k', A)$ by the rule $a'(\cdots, \sigma', \cdots) = a(\cdots, \sigma'_K, \cdots)$, where σ'_K denotes the effect on K of $\sigma' \in G(K'/k')$. The cochain map $a \rightarrow a'$ induces a homomorphism

$H^r(K/k, A) \to H^r(K'/k', A)$ which we simply call the *canonical* homomorphism. However, in the extreme case $k = k'$, it goes by the name of *inflation* (inf), and in the other extreme case $K = K'$, it is known as *restriction* (res).

PROPOSITION 1. *Let K/k be Galois and let k' be an arbitrary subfield. Then*

$$H^r(K/k', A) = \lim_{\substack{\rightarrow \\ F}} \{H^r(F/F \cap k', A)\},$$

the limit being taken inductively with respect to the canonical homomorphisms, as F runs over the finite subextensions of K.

Since passage to (co)homology commutes with inductive limits (cf. [2], Ch. V, Prop. 9.3*), our proposition will follow if we can show that the corresponding formula holds for the cochain groups. Each of the canonical maps $C^r(F/F \cap k', A) \to C^r(K/k', A)$ is an injection, because the inclusion $A(F \cap k') \to A(k')$ is injective and the natural map $G(K/k') \to G(F/F \cap k')$ is surjective. Thus we have only to show that each element $a \in C^r(K/k', A)$ is in the image of $C^r(F/F \cap k', A)$ for some F depending on a. Since a is of finite type, it has only a finite set of distinct values and by Axiom (A1), it follows that we can find a finitely generated, hence finite, sub-extension F/k of K/k such that all valuesof a lie in $A(F)$. Enlarging F, if necessary, so that $a(\sigma_1, \cdots, \sigma_r)$ depends only on the effects of the σ_i on Fk', we can well-define a cochain $b \in C^r(F/F \cap k', A)$ whose image is a by putting $b(\cdots, \sigma_F, \cdots) = a(\cdots, \sigma, \cdots)$, where σ_F denotes the effect of σ on F.

Taking the special case $k' = k$, we find as a corollary

$$H^r(K/k, A) = \lim_{\substack{\rightarrow \\ F}} \{H^r(F/k, A)\} = \lim_{\substack{\rightarrow \\ F}} \{H^r(G(F/k), A(F))\}.$$

Thus our cohomology groups are just the inductive limits, under inflation, of the ordinary cohomology groups of the finite subextensions.

Let L/K be a Galois extension. A k-isomorphism $\phi: L \to L^\phi$ induces an isomorphism $C(L/K, A) \to C(L^\phi/K^\phi, A)$ by the rule $a^\phi(\cdots, \sigma, \cdots) = \phi a(\cdots, \phi^{-1}\sigma\phi, \cdots)$, and it is a fact that the induced cohomology map $H^r(L/K, A) \to H^r(L^\phi/K^\phi, A)$, called *conjugation,* depends only on the effect of ϕ on K. In particular, if L and K are Galois extensions of k, then the Galois group $G(K/k)$ operates on $H^r(L/K, A)$.

Although there is no doubt that the whole spectral sequence of Hochschild-Serre carries over to the case of infinite Galois extensions we are content here to discuss only a small corner of it, namely:

PROPOSITION 2. *Let $K \supset k'$ be Galois extensions of k. Then there exists* *a canonical transgression homomorphism* (tg) *such that the following sequence is exact:*

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(K/k, A) \xrightarrow{\text{res}} H^1(K/k', A)^{G(k'/k)}$$
$$\xrightarrow{\text{tg}} H^2(k'/k, A) \xrightarrow{\text{inf}} H^2(K/k, A).$$

Indeed, this proposition is known in the case of ordinary cohomology groups (Cf. Hochschild, G. and Serre, J-P., "Cohomology of Group Extensions," *Trans. A. M. S.*, Vol. 74, 1953). Consequently, for each finite Galois subfield F of K, we have, exactly, with obvious abbreviations of notation:

$$0 \to H^1(F \cap k'/k) \to H^1(F/k) \to H^1(F/F \cap k')^{G(F \cap k'/k)}$$
$$\xrightarrow{\text{tg}} H^2(F \cap k'/k) \to H^2(F/k).$$

The commutativities required for passing to the inductive limit over F are satisfied and, by Proposition 1, the limit sequence is the one we are looking for. The superscript G on the middle term carries over to the limit because each $(F \cap k'/k)$ is finite.

It is easy to see that our limiting transgression map cap be characterized in the same way as the ordinary one, namely, we have $\alpha = \text{tg}\,\beta$ if and only if there is a cochain $b \in C^1(K/k, A)$ whose restriction to $C^1(K/k', A)$ is a cocycle representing β and whose coboundary δb is the inflation to $C^2(K/k, A)$ of a cocycle $a \in C^2(k'/k, A)$ representing α.

If K/k is Galois and E a finite (not necessarily Galois) subextension, there exists a *transfer* map

$$\text{tr}: H^r(K/E, A) \to H^r(K/k, A)$$

going in the opposite direction from restriction, whose definition we recall here, although we have little use for it in the sequel. Let Φ be the set of $[E:k]$ distinct k-isomorphisms of E. For each $\phi \in \Phi$, let $\phi_* \in G(K/k)$ be a chosen prolongation of ϕ to K. Then for $\sigma \in G(K/k)$, both $\sigma\phi_*$ and $(\sigma\phi)_*$ have the same effect on E, and, consequently, the automorphism $(\sigma\phi)_*^{-1}\sigma\phi_*$, which we shall denote by (σ, ϕ) leaves E elementwise fixed, i.e. belongs to $G(K/E)$. The cohomology transfer is that induced by the cochain transfer $a \to \text{tr}(a)$ defined by

$$(\text{tr}(a))(\sigma_1, \cdots, \sigma_r)$$
$$= \sum_{\phi \in \Phi} (\sigma_1\sigma_2 \cdots \sigma_r\phi)_* a((\sigma_1, \sigma_2 \cdots \sigma_r\phi),\ (\sigma_2, \sigma_3 \cdots \sigma_r\phi), \cdots, (\sigma_r, \phi)).$$

Although this cochain transfer depends on the choice of prolongations, the induced cohomology map does not. The main relation between transfer and restriction is the rule $\operatorname{tr} \circ \operatorname{res} = [E : k]$. This and all other such relations can be guessed from the case of dimension 0, where the transfer $A(E) \to A(k)$ is just the *trace*: $a \to \sum \phi a$, and the restriction $A(k) \to A(E)$ is just the inclusion map.

The relation $\operatorname{tr} \circ \operatorname{res} = [E : k]$ shows that if an element $\alpha \in H^r(K/k)$ restricts to 0 in $H^r(K/E)$, then $[E : k]\alpha = 0$. Applying this remark in case $E = K$ is a finite Galois extension of k, we see that $H^r(E/k)$ is a torsion group of exponent $[E : k]$ for $r > 0$, because $H^r(E/E, A) = 0$ for positive r. From Proposition 1, it now follows that the Galois cohomology groups in positive dimension are torsion groups for arbitrary K/k.

We conclude this section by considering the cohomology maps induced by a *homomorphism* $f : A \to B$ of one of our functors into another. By this we mean a collection of homomorphisms $f(K) : A(K) \to B(K)$ satisfying

(f1) If $L \supset K$, then $f(K)$ is the restriction of $f(L)$ to $A(K)$.

(f2) If $\phi : K \to K^\phi$ is a k-isomorphism, then

$$f(K^\phi) \circ A(\phi) = B(\phi) \circ f(K).$$

For example, suppose A and B are algebraic groups defined over k. Then a k-homomorphism $f : A \to B$ (that is, an everywhere defined rational map over k which is a group homomorphism) yields a homomorphism of the functor A into the functor B. We simply let $f(K)$ denote the restriction of f to $A(K)$. Condition (f2) is satisfied because f is defined over k.

A functor homomorphism $f : A \to B$ gives rise to cohomology homomorphisms

$$H^r(K/k, A) \to H^r(K/k, B),$$

namely, those induced by the cochain map $a \to f \circ a$, and these induced cohomology maps obviously commute with canonical maps, conjugations, and transfers. A sequence of functor homomorphisms $A' \to A \to A''$ is said to be *K-exact* if the sequence $A'(K) \to A(K) \to A''(K)$ is exact in the ordinary sense.

PROPOSITION 3. *Let K/k be Galois. A K-exact sequence*

$$0 \to A' \to A \to A'' \to 0$$

gives rise to an infinite exact cohomology sequence

$$\cdots \to H^r(K/k, A) \to H^r(K/k, A'') \xrightarrow{\delta} H^{r+1}(K/k, A') \to H^{r+1}(K/k, A) \to \cdots.$$

This proposition follows as usual from the lemma: *If $A' \to A \to A''$ is K-exact, then the cochain sequence*

$$C(K/k, A') \to C(K/k, A) \to C(K/k, A'')$$

is exact. If a cochain $a \in C(K/k, A)$ goes to 0 in $C(K/k, A'')$, then each of its values goes to 0 in $A''(K)$. Hence, by K-exactness, we can pick a pre-image in $A'(K)$ for each of these values and thereby define a cochain a' whose image is a. Moreover, a' will be of finite type, provided we select one single pre-image for each of the distinct values of a, because of Axiom (A1).

In many applications, we shall deal with the case where K is the separable closure k_s of k, and where the sequence of Proposition 3 is k_s-exact. The resulting cohomology sequence involves the cohomology groups $H^r(k_s/k, A)$ which we shall simply write $H^r(k, A)$ since they occur so frequently.

Such a sequence arises from commutative algebraic groups. As a matter of notation, if X is an abelian group and m a natural number, we shall denote by X_m the kernel of the map $X \xrightarrow{m} X$. Let A be a commutative group variety defined over k. If m is prime to the characteristic, the sequence

$$0 \to A_m \to A \xrightarrow{m} A \to 0$$

is k_s-exact. Writing A_K instead of $A(K)$, our cohomology sequence becomes

$$0 \to A_m \cap A_k \to A_k \xrightarrow{m} A_k \to H^1(k, A_m) \to H^1(k, A) \xrightarrow{m} H^1(k, A) \to \cdots.$$

A portion of this exact sequence may be written more simply as follows.

$$0 \to A_k/mA_k \to H^1(k, A_m) \to H^1(k, A)_m \to 0.$$

The group A_k/mA_k is well known to be of interest in arithmetical questions, and we shall investigate it from this point of view in § 5. For the moment, we assume further that $A_m \subset A_k$, and let G_k be the Galois group of k_s over k, i. e. $G_k = G(k_s/k)$. Then G_k operates trivially on A_m, and our sequence becomes

$$0 \to A_k/mA_k \to \operatorname{Hom}(G_k, A_m) \to H^1(k, A)_m \to 0,$$

where Hom means, of course, the continuous homomorphisms as always. We shall have many applications for this sequence, and we shall call it the *Kummer* sequence, because, in case A is the multiplicative group, we have

$H^1(k, A) = 0$ by Hilbert's Theorem 90, so that we find the familiar Kummer duality

$$k^*/k^{*m} \approx \operatorname{Hom}(G_k, A_m),$$

always provided that the group of m-th roots of unity A_m is contained in $A_k = k^*$.

2. Principal homogeneous spaces. Let A be a functor of the type described in the first paragraph of § 1. If the groups $A(K)$ are not commutative, we cannot define cohomology groups $H^r(K/k, A)$ for Galois extensions K/k. The best we can do is define cohomology *sets* in dimension *one*, as follows. We consider 1-cochains a of finite type and we call 1-cycles those satisfying the identity $a_\sigma a_\tau{}^\sigma = a_{\sigma\tau}$. Here we write $A(K)$ multiplicatively and write a_σ instead of $a(\sigma)$ for $\sigma \in G(K/k)$. We do not attempt to multiply 1-cocycles, but we explain when two 1-cocycles a and a' are cohomologous, namely, when there exists an element $b \in A(K)$ such that $a'_\sigma = b^{-1} a_\sigma b^\sigma$. The cohomology thus defined is an equivalence relation, and we denote the set of equivalence classes by $H^1(K/k, A)$. This set is not a group but it does have a distinguished element, namely the class of coboundaries of the form $a_\sigma = b^{-1} b^\sigma$, which we call the trivial class.

The reader will easily verify that the canonical maps, in particular, restriction and inflation, the conjugation maps, and the induced maps make sense for this non-commutative cohomology.

Proposition 1 holds in dimension 1.

Proposition 2 holds in a weaker form, namely, in the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(K/k, A) \xrightarrow{\text{res}} H^1(K/k', A)^{G(k'/k)}$$

inf is an injection whose image is the inverse image of the trivial class under restriction.

Proposition 3 collapses to the exactness of the sequence

$$0 \to A(k) \to B(k) \to C(k) \xrightarrow{\delta} H^1(K/k, A) \to H^1(K/k, B) \to H^1(K/k, C),$$

where we now deal with a K-exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

Here exactness means that the image of each map is the inverse image of the trivial element under the succeeding map, and there is the additional feature that δ injects the right coset space $C(k)/gB(k)$ into $H^1(K/k, A)$.

Suppose now that A is a group variety defined over k. We wish to explain the connection between the 1-dimensional cohomology sets and the right principal homogeneous spaces for A. To recall the definition of this latter object, a right phs for A over k is a variety V defined over k on which A operates simply and transitively, in such a way that the map $(v, w) \rightarrow v^{-1}w$ of $V \times V$ into A is an everywhere defined rational map over k. Here we use the symbol $v^{-1}w$ to denote the uniquely determined element of A which carries the point v into the point w, so that the formula $v(v^{-1}w) = w$ becomes an identity. Two phs's V and V' are said to be *k-isomorphic* if there exists a birational biholomorphic transformation $f\colon V \rightarrow V'$ such that $f(va) = f(v)a$ for $v \in V$ and $a \in A$. Among the k-isomorphism classes, there is a distinguished class, namely, the class of spaces which are k-isomorphic to A itself, viewed as phs under right multiplication. A space is in this class if and only if it has a rational point in k. In case A is commutative, Weil [13] has defined a geometric law of composition which makes the classes of phs's into a commutative group.

The following proposition has been proved by F. Chatelet [3], [4] for various special groups.

PROPOSITION 4. *Let K/k be a Galois extension. There is a canonical bijection between the first cohomology set $H^1(K/k, A)$ and the set of k-isomorphism classes of principal homogeneous spaces for A over k which have rational points in K. This bijection is a group isomorphism when A is commutative.*

Proof. Let V be a phs with a rational point v in K. Each such point gives rise to a 1-cocyle $a_\sigma = v^{-1}v^\sigma$. The different choices of v lead to cocycles filling out a cohomology class. Denote this class by $\alpha(V)$. If V and V' are k-isomorphic, then points v and v' which correspond under a k-isomorphism yield the same cocycle; hence $\alpha(V) = \alpha(V')$. Conversely, if V and V' are given such that $\alpha(V) = \alpha(V')$, then there do exist points v and v' yielding the same cocycle. When this is the case, the map $x \rightarrow v'(v^{-1}x)$ is a k-isomorphism of V onto V'. Indeed, it is a K-isomorphism, and a simple computation shows that it is invariant under all $\sigma \in G(K/k)$. We have thus obtained an injection of the classes of spaces into the cohomology set.

As Serre has observed, it follows immediately from Weil's theorems concerning the field of definition of a variety that every cocycle comes from a space. Indeed, consider the transformations $f_\sigma : A \to A$ defined by $f_\sigma(x) = a_\sigma x$. They satisfy the identity $f_\sigma \circ f_\tau{}^\sigma = f_{\sigma\tau}$. Since the cocycle a is of finite type, it follows from [14] that there exists a variety V defined over k and a birational biholomorphic transformation $F : A \to V$ defined over K such that $f_\sigma = F^{-1} \circ F^\sigma$. The operation $vb = F(F^{-1}(v)b)$ for $v \in V$ and $b \in A$ makes V into a phs for A over k, not only over K, because a simple computation shows that $(v^{-1}w)^\sigma = ((v^\sigma)^{-1}w^\sigma)$. Finally, one sees that the cocycle a with which we started is that arising from the point $v = F(1)$ on V.

If A is commutative, let U, V, W be phs's and suppose $f : U \times V \to W$ is an everywhere defined rational map over k which exhibits the fact that the class of W is the product of the classes of U and V (cf. [13], prop. 5). Select $u \in U$, $v \in V$ rational over K and put $w = f(u, v)$. Using the characteristic property of f, namely $f(ua, vb) = f(u, v)ab$, one finds that the cocycle derived from w is the product of those derived from u and v. This concludes the proof.

Since every variety defined over k has a point whose coordinates lie in the separable algebraic closure k_s of k, it follows from Proposition 4 that the set (group) of all principal homogeneous spaces for A over k is isomorphic to $H^1(k_s/k, A)$ which we have agreed to write $H^1(k, A)$, and which we shall call the *Chatelet set* (*group*) for A over k.

If k' is an extension field of k, it is obvious that the canonical cohomology map $H^1(k, A) \to H^1(k', A)$ reflects the homogeneous space operation of extending the ground field from k to k'. The cohomology classes in the kernel of this map are said to be *split* by k', and the same terminology is applied to the corresponding homogeneous spaces. Thus a phs for A over k is *split* by an extension k' if and only if it is k'-isomorphic to A, or what is the same, if and only if it has a rational point in k'. In case k'/k is a Galois extension, the exactness of the sequence

$$0 \to H^1(k'/k, A) \xrightarrow{\text{inf}} H^1(k, A) \xrightarrow{\text{res}} H^1(k', A)$$

is obvious from the point of view of homogeneous spaces, for the cohomology inflation map simply reflects the inclusion of the set of phs's split by k' in the set of all phs's for A over k.

Let X be a variety defined over k. We define the *index* of X over k ($\operatorname{ind} X$) to be the greatest common divisor of the degrees of the 0-cycles on X which are prime rational over k. The degree of a prime rational 0-cycle is equal to the degree of the extension generated over k by the coordinates of one of its points. Thus, in the case of a principal homogeneous space V

for A over k, we see that ind V is the greatest common divisor of the degrees of the finite extensions of k which split V, and is consequently subject to a cohomological analysis.

From now on, we assume that A is commutative. Defining the *separable index* of V ($\mathrm{ind}_s V$) as the greatest common divisor of the degrees of the finite separable splitting extensions, and the *period* of V ($\mathrm{per}\, V$) as the period of V in the group of classes of principal homogeneous spaces for A over k, we have

PROPOSITION 5. *Let V be a principal homogeneous space for A over k. Then* $\mathrm{per}\, V$ *divides* $\mathrm{ind}\, V$ *divides* $\mathrm{ind}_s V$, *and all three numbers have the same prime factors.*

Proof. It is trivial that the index divides the separable index. Let v_0 be a rational point of V in some Galois extension of k. Let $f\colon V \rightarrow A$ be the map $v \rightarrow v_0^{-1}v$, and let $a_\sigma = v_0^{-1}v^\sigma$ be the cocycle determined by v_0. Then for any point $v \in V$, we have $a_\sigma(f(v))^\sigma = f(v^\sigma)$, and consequently, by linearity, we have

$$a_\sigma^{\deg(\mathfrak{d})}(f(\mathfrak{d}))^\sigma = f(\mathfrak{d}^\sigma)$$

for any 0-cycle $\mathfrak{d}$ on V. If $\mathfrak{d}$ is rational over k and of degree d, then $\mathfrak{d}^\sigma = \mathfrak{d}$, and the d-th power of the cocycle a_σ is split by the coboundary of $f(\mathfrak{d})$. This proves that the period divides the index.

Finally, let p be a prime number not dividing the period. We must show that p does not divide the separable index, that is, we must construct a finite separable splitting extension E_p whose degree is not divisible by p. To this effect, we simply take any finite Galois splitting extension K/k and let E_p be the subextension cut out by a p-Sylow subgroup of $G(K/k)$. If $\alpha \in H^1(K/k, A)$ is the cohomology class of V, then the period of $\mathrm{res}\,\alpha \in H^1(K/E, A)$ divides the p-power $[K:E]$ on the one hand, and divides $\mathrm{per}\, V$ on the other. Consequently, $\mathrm{res}\,\alpha = 0$, i.e. E splits V.

The reader will have noticed the analogy between the Chatelet group of classes of principal homogeneous spaces for A over k and Brauer's group of classes of central simple algebras over k. We have in fact taken over Proposition 5 and its proof almost word for word from the theory of algebras. In the case of algebras, the period is not in general equal to the index as a counterexample of Albert [1] shows. We have found a similar counterexample in the case of principal homogeneous spaces (end of § 4). Nevertheless, our counterexample, like Albert's, involves a comparatively complicated ground field k, and over number fields and their completions, all examples which we have satisfy the condition period $=$ index.

The theory of algebras suggests other questions. Since every central division algebra contains a separable splitting field, it is true for algebras that (1) the index equals the separable index, and (2) the index is not only the greatest common divisor, but is actually the minimum of the degrees of the finite splitting fields. We have not investigated the corresponding statements for homogeneous spaces, except to notice that (2) is true in case A is an elliptic curve, for in that case, the Riemann-Roch theorem shows that every divisor class of positive degree contains positive diivsors.

The divisibilities of Proposition 5 imply

COROLLARY. *Suppose $\alpha \in H^1(k, A)$ is of period m and is split by an extension E/k of degree m. Then the corresponding homogeneous space has index m.*

This corollary will enable us to construct, with abelian varieties A, over various ground fields k, examples of spaces whose index is a preassigned integer m (cf. Theorem 7, § 5). These examples are of particular interest in case A is an elliptic curve. Then V, which becomes birationally equivalent to A over an extended ground field, is also a curve of genus 1. The point is that the index of a curve of genus $g \neq 1$ is bounded by, and in fact divides, $2g-2$, for the Riemann-Roch theorem shows the existence of divisors rational over k of degree $2g-2$. On the other hand, our examples show that the index is completely arbitrary for $g=1$, a fact conjectured by Artin, but unknown until now.

3. Non-degenerate reduction. Throughout this section, we assume that we have a field k and a place of k onto a field k' such that any two extensions of it to the algebraic closure $\bar{k}$ of k are conjugate over k'. In terms of valuations, this means that the extension of the valuation is unique, and this condition is certainly satisfied if k is complete, and the valuation discrete.

We denote by θ a definite extension of our place to $\bar{k}$. An automorphism σ of $G(\bar{k}/k)$ induces an automorphism σ' of the algebraic closure of k', characterized by the relation $\theta\sigma = \sigma'\theta$. The map $\sigma \to \sigma'$ is a homomorphism of $G(\bar{k}/k)$ onto $G(\bar{k}'/k')$.

We shall also assume that the valuation is discrete, although this can presumably be dispensed with. If Z is a cycle rational over an algebraic extension K of k (say in some projective space), then it has a reduction, or, as we shall also say, a specialization Z' in the reduced projective space determined by θ, and rational over K' (Shimura [12]). The only facts concerning the specialization $Z \to Z'$ which we shall use in the sequel is that it commutes with projections and intersections, i.e. under suitable hypotheses, $(\mathrm{pr}\, Z)' = \mathrm{pr}(Z')$, and for two positive cycles X, Y, we have $(X \cdot Y)' = X' \cdot Y'$. We refer to [12] for the proof.

Our place θ induces a mapping of points P of our projective space, algebraic over k, onto points P', algebraic over k'. We shall also write $P' = \theta P$. We have for any automorphism σ of $\bar{k}/k$, $(\sigma P)' = \sigma' P'$. If Z is a positive cycle, then $\mathrm{supp}(Z') = (\mathrm{supp}\, Z)'$.

We shall now list a few properties of reduction of cycles, and especially varieties in non-degenerate cases.

To begin with, we have a result which will serve as Hensel's lemma for points on varieties.

LEMMA. *Let $\mathfrak{a}$ be a positive 0-cycle rational over k. Let P' be a point of $\mathfrak{a}'$ which occurs in $\mathfrak{a}'$ with multiplicity* 1. *Then there exists a unique point P of $\mathfrak{a}$ specializing to P', and P is rational over k.*

Proof. Note that P' is rational over k' since $\mathfrak{a}'$ is rational over k'. Let P be in $\mathfrak{a}$, specializing to P'. Then obviously P occurs with multiplicity 1, so that P is separable over k. If σ is any automorphism of $\bar{k}$ over k, then $(\sigma P)' = (\sigma' P') = P'$, and hence σP also specializes to P'. Since $\mathfrak{a}$ is rational over k, it follows that σP also occurs in $\mathfrak{a}$, and since P' has multiplicity 1, we conclude that $\sigma P = P$, and hence that P is rational over k.

We now have the surjectivity of θ, whose proof is due to Chow.

PROPOSITION 6. *Let the cycle Z be a variety V, and assume that Z' is also a variety V', i.e. consists of one component with multiplicity* 1. *Let P' be a simple point of V', rational over k'. Then there exists a point P of V rational over k which specializes to P'.*

Proof. Our statement being local, we may assume that V' is affine. There exists a linear variety L' defined over k' such that $V' \cdot L'$ is defined and contains P' with multiplicity 1. Lift L' to a linear variety L over k, such that $V \cdot L$ is defined. Then $V \cdot L$ contains a point P specializing to P'. Since $V \cdot L$ is rational over k, we need merely apply the lemma and the compatibility of specializations with intersections to conclude the proof.

For the applications, we are principally interested in abelian varieties. Let A be an abelian variety defined over k. Its specialization A' is then a cycle. If this cycle has one component with multiplicity 1, which is an abelian variety whose law of composition is obtained by reduction of that of A, then we shall say that the specialization $A \to A'$ is *non-degenerate*. (The uniqueness of non-degenerate specializations has been proved in [5].) In that case, if a, b are two points of A algebraic over k, then $(a + b)' = a' + b'$, the first + referring to addition on A and the second on A'. In view of Proposition 6, we have an exact sequence

$$0 \to S_k \to A_k \to A'_{k'} \to 0,$$

where S_k is simply the kernel of the specialization homomorphism θ. If K is a finite Galois extension of k with group G then each one of the groups S_K, A_K, $A'_{K'}$ is a G-module, in view of the relation $(\sigma x)' = \sigma' x'$. It is to the exact sequence

$$0 \to S_K \to A_K \to A'_{K'} \to 0$$

that we shall apply the cohomology theory in the next section.

Suppose for a moment that k is a p-adic field $\boldsymbol{Q}_p$ and A is an elliptic curve of the type considered by Lutz [8]. Then A_k contains a subgroup isomorphic to the integers of $\boldsymbol{Q}_p$, which is none other than our kernel S_k when A' is non-degenerate. More generally, if k is an arbitrary $\mathfrak{p}$-adic field, and A an abelian variety of dimension r, then Mattuck [9] has shown that A_k contains a subgroup isomorphic to r copies of the integers of k. We can always choose such a subgroup M_k of Lutz-Mattuck such that $M_k \subset S_k$. We shall prove below that S_k is uniquely divisible by an integer m prime to p. From this one sees that $(S_k : M_k)$ is a power of p.

We return to an arbitrary field k subject to the conditions stated at the beginning of this section. Let m be an integer not divisible by the characteristic p of k'. Let a be a point of A rational over k. The cycle

$$(m\delta)^{-1}(a) = \mathrm{pr}_1\{\Gamma \cdot (A \times (a))\},$$

where Γ is the graph of $m\delta$, consists of the points x on A such that $mx = a$, each one occurring with multiplicity 1. Specializing, we see that

$$[(m\delta)^{-1}(a)]' = (m\delta')^{-1}(a'),$$

where δ' is the identity on A'. Taking $a = 0$, this shows in particular that θ induces an isomorphism of the points of finite order prime to p on A onto those points on A', i.e. of A_m onto A'_m. Actually, from Hensel's lemma, we get

PROPOSITION 7. *Assume that the specialization* $A \to A'$ *is non-degenerate. Let* m *be an integer prime to* p. *Then the homomorphism* θ *induces an isomorphism of* $A_m \cap A_k$ *onto* $A'_m \cap A'_{k'}$.

Furthermore, we also get information concerning the kernel S_k in our exact sequence above.

PROPOSITION 8. *Assume that the specialization* $A \to A'$ *is non-degenerate. Let* m *be an integer prime to* p. *Then* S_k *is uniquely divisible by* m.

Proof. Let a be in S_k, so that $a' = 0'$. The cycle $(m\delta)^{-1}(a)$ specializes to the cycle $(m\delta')^{-1}(a') = (m\delta')^{-1}(0')$ which consists of the points of order m on A'. Since $(0')$ occurs with multiplicity 1 in the reduced cycle, it follows by Hensel's lemma that there is exactly one point on $(m\delta)^{-1}(a)$ which specializes to $0'$ and that this point is rational over k.

PROPOSITION 9. *Assume that the specialization $A \rightarrow A'$ is non-degenerate. Let m be an integer prime to p. Let a be a point of A_k, and let $K = k(1/m \cdot a)$ be the field obtained by adjoining all points x such that $mx = a$. Then K is unramified over k, and $K' = k'(1/m \cdot a')$.*

Proof. This is again an immediate consequence of Hensel's lemma. Taking into account the fact that the points in $(m\delta')^{-1}(a')$ are all separable over k', we see that K is in fact the uniquely determined unramified extension of k such that $K' = k'(1/m \cdot a')$.

We conclude this section by a remark on the reduction of principal homogeneous spaces. Let V be such a space over A, defined over k. Suppose that V' has one component with multiplicity 1. Then V' has a simple rational point in some separable extension of k', and hence, by Proposition 6, V has a point in, and is split by, an unramified extension of k.

4. Cohomology and non-degenerate reduction. Let k be a field complete with respect to a discrete valuation and let A be an abelian variety defined over k which has a non-degenerate reduction A' modulo the prime in k. The only fields we consider are the algebraic extensions K of k and their residue class fields K'. From the preceding section we know the following facts:

(R1) The reduction map $\theta_K\colon A_K \rightarrow A'_{K'}$ is surjective for each K and its kernel S_K is uniquely divisible by an integer m prime to the residue class characteristic, p.

(R2) If K' is separably closed, then $A'_{K'}$ is divisible by m and contains A'_m for m prime to p.

The following cohomological analysis makes no reference to the details of the reduction process itself, nor even to abelian varieties. It applies to any pair of commutative functors A and A' of the fields K and K' (in the sense of § 1) which are linked by a natural homomorphism $\theta\colon A \rightarrow A'$ so that conditions (R1) and (R2) are satisfied. Note that (R1) implies, trivially,

(R1′) θ_K induces a bijection $A_m \cap A_K \rightarrow A'_m \cap A'_{K'}$ for each K, and m prime to p.

Let k_u denote the maximal unramified extension of k. Then the residue class field of k_u is the separable closure of the residue class field of k, or in symbols, $(k_u)' = (k')_s$.

For the rest of this section, we let m be an integer prime to p. Our goal is now Theorem 1 below.

LEMMA 1. *If $K \supset k_u$, then A_K is divisible by m and contains A_m.*

Proof. K' is separably closed because $K \supset k_u$. Hence, by (R2), we know the divisibility by m of the factor group $A_K/S_K \approx A'_{K'}$. Since from (R1), we know S_K is also divisible by m, we conclude that A_K is. We also know from (R2) that $A'_m \subset A'_{K'}$. This together with (R1′) implies that $A_m \cap A_K$ is independent of K for $K \supset k_u$, and consequently, $A_m \subset A_K$.

The group Ω_m of m-th roots of unity is contained in k_u, and the group of units in k_u is divisible by m. Therefore the maximal abelian extension of k_u of exponent m is the field $k_u(\pi^{1/m})$ obtained by adjoining the m-th root of any prime element π of k_u. The Galois group of this extension is canonically isomorphic to Ω_m. Indeed, the map $\sigma \rightarrow \zeta_\sigma = (\pi^{1/m})^{\sigma-1}$ is a homomorphism of G_{k_u} onto Ω_m, whose kernel cuts out $k_u(\pi^{1/m})$, and this homomorphism is independent of π and its chosen m-th root.

LEMMA 2. *There is a canonical isomorphism*

$$\operatorname{Hom}(\Omega_m, A_m) \approx H^1(k_u, A)_m$$

which attaches to each homomorphism $\chi\colon \Omega_m \rightarrow A_m$ the cohomology class of the cocycle $\sigma \rightarrow \chi(\zeta_\sigma)$, $\sigma \in G(k_s/k_u)$.

Proof. Since A_{k_s} is divisible by m, the Kummer sequence at the end of § 1 is applicable, and since A_{k_u} is divisible by m, it yields an isomorphism

$$\operatorname{Hom}(G_{k_u}, A_m) \approx H^1(k_u, A)_m.$$

Since A_m is commutative of exponent m, any homomorphism $h\colon G_{k_u} \rightarrow A_m$ will have the property that $h(\sigma)$ depends only on the effect of σ on an abelian extension of exponent m. Consequently, according to the discussion preceding this lemma, we can factor h through $\sigma \rightarrow \zeta_\sigma$, i.e. we can write $h(\sigma) = \chi(\zeta_\sigma)$ for some $\chi\colon \Omega_m \rightarrow A_m$.

The Galois group G_k of k_s/k operates on $H^1(k_u, A)$ as explained in § 1. It also operates on Ω_m and on A_m, and consequently, on $\operatorname{Hom}(\Omega_m, A_m)$ in the usual manner, so that

$$(\chi^\phi)(\zeta^\phi) = \phi(\chi(\zeta))$$

for $\phi \in G_k$.

LEMMA 3. *The isomorphism of Lemma 2 is a G_k-isomorphism.*

Proof. Let $\chi \in \operatorname{Hom}(\Omega_m, A_m)$ and let $a_\sigma = \chi(\zeta_\sigma)$ be the corresponding cocycle. Let $\phi \in G_k$. Then for $\sigma \in G_{k_u}$, we have

$$(a^\phi)_\sigma = \phi a_{\phi^{-1}\sigma\phi} = \phi\chi(\zeta_{\phi^{-1}\sigma\phi}) = \chi^\phi(\zeta_{\phi^{-1}\sigma\phi}{}^\phi) = \chi^\phi(\zeta_\sigma)$$

because

$$\zeta_{\phi^{-1}\sigma\phi}{}^\phi = (\pi^{1/m})^{\sigma\phi-\phi} = ((\pi^\phi)^{1/m})^{\sigma-1} = \zeta_\sigma.$$

Note that because of the way G_k is defined to operate on $\operatorname{Hom}(\Omega_m, A_m)$, we have

$$\operatorname{Hom}(\Omega_m, A_m)^{G_k} = \operatorname{Hom}_{G_k}(\Omega_m, A_m)\,;$$

in other words, a homomorphism is left fixed by the operation of G_k if and only if it is a G_k-isomorphism.

LEMMA 4. *The sequence*

$$0 \to H^1(k_u/k, A)_m \xrightarrow{\text{inf}} H^1(k, A)_m \xrightarrow{\text{res}} [H^1(k_u, A)_m]^{G_k} \to 0$$

is exact.

Proof. Of course, it is only necessary to prove that the restriction is surjective. By the preceding lemmas, an element $\alpha \in H^1(k_u, A)_m$ which is invariant under G_k will be represented by a cocycle of the form $a_\sigma = \chi((\pi^{1/m})^{\sigma-1})$, $\sigma \in G_{k_u}$, where $\chi\colon \Omega_m \to A_m$ is a G_k-homomorphism. Here π is an arbitrary prime in k_u. Choosing π in k, and choosing a definite m-th root, we see that that the expression for a_σ makes sense for all $\sigma \in G_k$, not only for $\sigma \in G_{k_u}$. Now

$$\sigma \to (\pi^{1/m})^{\sigma-1}$$

is a cocycle in Ω_m (it is a coboundary in Ω), and since $\chi\colon \Omega_m \to A_m$ is a G_k-homomorphism, it follows that a_σ is still a cocycle. By construction, its class $\beta \in H^1(k, A)_m$ restricts to α.

Since k_u/k is unramified, its Galois group may be identified with the Galois group of its residue class extension. We shall make this identification from now on, and will designate both groups by the simpler symbol $G_{k'}$. Of course, $\theta\colon A_{k_u} \to A'_{k'}$, is a $G_{k'}$-homomorphism.

LEMMA 5. *θ induces an isomorphism $H^1(k_u/k, A)_m \approx H^1(k', A')_m$.*

Proof. Since A_{k_u} and A'_{k_s} are divisible by m, we can apply the Kummer sequence to the extensions k_u/k and k'_s/k', obtaining the exact horizontal rows in the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_k/mA_k \arrow[r] \arrow[d, "\theta"'] & H^1(k_u/k, A_m) \arrow[r] \arrow[d, "\theta"'] & H^1(k_u/k, A)_m \arrow[r] \arrow[d, "\theta"'] & 0 \\
0 \arrow[r] & A'_{k'}/mA'_{k'} \arrow[r] & H^1(k', A'_m) \arrow[r] & H^1(k', A')_m \arrow[r] & 0
\end{tikzcd}$$

The left vertical arrow is surjective by (R1). The middle is bijective because A_m is $G_{k'}$-isomorphic to A'_m (recall that $G_k = G(k_u/k)$). Consequently, the right vertical arrow is bijective as contended.

Putting our results together, we see that we have proved a good part of

THEOREM 1. *Let k be a field complete with respect to a discrete valuation with residue class field k' of characteristic $p \geqq 0$. Let A and A' be two commutative functors as in § 1, satisfying* (R1) *and* (R2). *Then for each natural number m not divisible by p, there exists a canonical exact sequence*

$$0 \to H^1(k', A')_m \to H^1(k, A)_m \to \operatorname{Hom}_{G_{k'}}(\Omega'_m, A'_m) \to 0,$$

where Ω'_m is the group of m-th roots of unity in the residue field. Furthermore, if K is a finite extension of k with ramification index e, the following diagram is commutative:

$$\begin{tikzcd}
H^1(k', A')_m \arrow[r] \arrow[d, "\mathrm{res}"'] & H^1(k, A)_m \arrow[r] \arrow[d, "\mathrm{res}"'] & \operatorname{Hom}_{G_{k'}}(\Omega'_m, A'_m) \arrow[d, "e"'] \\
H^1(K', A')_m \arrow[r] & H^1(K, A)_m \arrow[r] & \operatorname{Hom}_{G_K}(\Omega'_m, A'_m).
\end{tikzcd}$$

Proof. The indicated exact sequence results from the preceding two lemmas and the trivial replacement of Ω_m and A_m by the isomorphic Ω'_m and A'_m. The commutativity of the left square is obvious. That of the right follows from the relationship

$$\chi((\pi^{1/m})^{\sigma-1}) = \chi^e((\pi_1{}^{1/m})^{\sigma-1})$$

for $\sigma \in G_{K_u}$, where π_1 is a prime in K_u and $\pi \sim \pi_1{}^e$ is a prime in k_u.

Naturally, we are interested here in the case where the functors are given by an abelian variety A defined over k, and a non-degenerate reduction A'. Theorem 1 gives especially precise information when $H^1(k', A') = 0$. This is the case, for example, if k' is algebraically closed, or finite [7]. Then we obtain simply an isomorphism

$$H^1(k, A)_m \approx \operatorname{Hom}_{G_{k'}}(\Omega'_m, A'_m).$$

From the commutative diagram of the theorem, we obtain the following corollaries.

COROLLARY 1. *Assume k' is either finite or algebraically closed. Let A be an abelian variety defined over k, with a non-degenerate reduction A'. Then a finite extension K/k splits an element $\alpha \in H^1(k, A)_m$ if and only if the ramification index $e(K/k)$ is divisible by the period of α.*

In terms of homogeneous spaces, this means that the homogeneous space

V corresponding to α has a rational point in K if and only if $e(K/k)$ is divisible by its period.

COROLLARY 2. *Let A, A' be as in Corollary 1. Let V be a principal homogeneous space of A defined over k, of period prime to p. Then the index of V is equal to its period.*

Proof. There exist ramified extensions, e.g. $k(\pi^{1/e})$, with preassigned ramification index, whose degree is equal to that index.

To describe $\operatorname{Hom}(\Omega'_m, A'_m)$ more concretely is, of course, easy. We choose a generator ζ for Ω'_m. Then a homomorphism χ is determined by the image $\chi(\zeta)$ of ζ, and this may be any element of A'_m. In order that χ be a $G_{k'}$-homomorphism, it is necessary and sufficient that $\chi(\zeta^\sigma) = \sigma\chi(\zeta)$ for each $\sigma \in G_{k'}$. Defining the integer $\nu_\sigma \pmod m$ by $\zeta^\sigma = \zeta^{\nu_\sigma}$, we see that the condition becomes $\nu_\sigma\chi(\zeta) = \sigma\chi(\zeta)$. Thus, $\operatorname{Hom}_{G_k}(\Omega'_m, A'_m)$ is isomorphic to the group of solutions $x \in A'_m$ of the equations $\sigma x = \nu_\sigma x$, $\sigma \in G_{k'}$. The isomorphism is not canonical, but depends on the choice of a primitive m-th root of unity ζ.

In particular, suppose that k' is a finite field with q elements. Then $G_{k'}$ has a canonical generator, namely the Frobenius automorphism $\xi \rightarrow \xi^q$. Its effect on an element x of A' is denoted by $x^{(q)}$. We may therefore express our result in this case as follows.

THEOREM 2. *Let A be an abelian variety defined over k with a non-degenerate reduction A', and suppose k' is a finite field with q elements. Then the group of elements of order prime to p in $H^1(k, A)$ is isomorphic to the group of solutions of $x^{(q)} = qx$ on A', of order prime to p.*

We observe that $x \rightarrow x^{(q)} - qx$ is an endomorphism of A'. Furthermore, if π denotes the Frobenius endomorphism of A', then its transpose ${}^t\pi$ on the Picard variety is easily seen to be given by the formula

$$ {}^t\pi y = qy^{(1/q)}. $$

Consequently, the transpose of $\pi - \delta$ is given by the endomorphism $y \rightarrow qy^{(1/q)} - y$ on $\hat{A}'$. Raising the kernel of this endomorphism to the q-th power, we see that the kernel is isomorphic to the subgroup of $\hat{A}'$ satisfying $y^{(q)} = qy$. In particular, we see that the group of solutions of $x^{(q)} = qx$ on A', of order prime to p, is dual to the group of rational points of $\hat{A}'$ in k', of order prime to p.

We close this section with an example of a homogeneous space whose index is not equal to its period. Suppose first of all that we could construct an abelian variety A over a field k such that $A_m \subset A_k$ and such that A_K is divisible by m for each algebraic extension K of k. Then the Kummer sequence gives isomorphisms

$$\mathrm{Hom}(G_k, A_m) \approx H^1(k, A)_m$$

and, moreover, for each K/k, a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(G_k, A_m) \arrow[r, phantom, "\approx"] \arrow[d, "\mathrm{res}"'] & H^1(k, A)_m \arrow[d, "\mathrm{res}"] \\
\mathrm{Hom}(G_K, A_m) \arrow[r, phantom, "\approx"] & H^1(K, A)_m,
\end{tikzcd}$$

where the left hand res means restriction of homomorphisms from G_k to G_K. If $f\colon G_K \to A_m$ is a homomorphism, we see that K splits the corresponding cohomology class if and only if G_K is in the kernel of f. Thus the index of the corresponding homogeneous space would be the *order* of the group $f(G_k)$, whereas its period would be the *exponent* of the group $f(G_k)$. In particular, if k has an abelian extension whose group is isomorphic to A_m, i.e. to the direct product of $2r$ cyclic groups of order m ($r = \dim A$), then we can construct a homogeneous space with index m^{2r} and period m.

An actual example can be constructed easily enough. Let A be defined over an algebraically closed field k_0. Define $k_i = k_{i-1}((t_i))$ (power series in one variable) for $1 \leqq i \leqq 2r$. One proves by induction that $A_{k_i} = mA_{k_i}$, and a similar divisibility statement for finite extensions. Then we can construct our example with $k = k_{2r}$ and the abelian extension $k(t_1^{1/m}, \cdots, t_{2r}^{1/m})$.

One could also construct a similar example over a purely transcendental function field in $2r$ variables. Incidentally, we note that the Kummer sequence shows, for any A and k, that if $A_m \subset A_k$ and $\mathrm{per}_k V = m$, then $\mathrm{ind}_k V$ divides m^{2r}. Thus our example is as bad as possible under the conditions $A_m \subset A_k$.

5. Global fields. Let k be a field with a fixed set of (inequivalent) discrete valuations $\mathfrak{p}$ which we shall call primes. By a prime in a finite algebraic extension K of k, we mean, of course, a valuation of K which extends a prime of k. Let m be a natural number not divisible by the characteristic of k. We shall say that k is an *m-global field* if each finite extension K of k has the following two properties.

(Gl1) If A is an abelian variety defined over K, then A has a non-degenerate reduction at all but a finite set of primes $\mathfrak{p}$ of K.

(Gl2, m) The set of primes of K dividing m is finite, and if S is any finite set of primes of K, there is only a finite number of abelian extensions of K of exponent m which are unramified outside S.

By well known elementary properties of number fields, one sees immediately that an algebraic number field of finite degree is m-global for every m, if we take as primes all the inequivalent discrete valuations.

The same remark applies to a field of algebraic functions of one variable over a finite constant field, and shows that it is m-global for m prime to its characteristic.

More generally, let k be an algebraic function field in n variables (the case $n = 0$ is not excluded) over a constant field k_0 such that $k_0{}^*/(k_0{}^*)^m$ is finite, for instance, a $\mathfrak{p}$-adic field, or an algebraically closed field. Choose as set of primes of k those arising from the prime divisors rational over k_0 of a projective normal model of k. Then it is easy to see (using results of algebraic geometry) that k is m-global.

Finally, if k is a function field over an algebraic number field of finite degree, then k is m-global for every m. The set of primes is then to be the set of prime divisors on a "mixed characteristic" model. This can easily be seen by reducing the proof to a geometric statement. As this, and the above fields are meant mostly to give concrete examples of m-global fields to the reader, we do not go in detail into the proofs that they are m-global, since they are essentially well known.

For the convenience of the reader, we indicate very briefly a sketch of the manner in which the above fields can be proved to satisfy our two global axioms.

(Gl 1) actually depends on the fact that an element of the field k has only a finite number of zeros and poles. To check that a reduction is non-degenerate, one checks that each property entering into the definition of an abelian variety has a non-degenerate reduction. For instance, we have: the absolute irreducibility (say of the Chow form if the variety is in projective space); the non-singularity (which depends on the non-vanishing of a determinant which is an element of k); the fact that some mappings are everywhere defined; associativity; etc.

As for (Gl 2), say for number fields, one may look at it either from the point of view that there is only a finite number of unramified extensions of degree m (abelian or non-abelian), a fact already stated in Hilbert's *Zahlbericht*, or from the point of view of Kummer theory: After adjoining the m-th roots of unity, the extension can be obtained by extracting radicals, and one uses the finiteness of class number and unit theorem. In the geometric case, one uses the analogous facts, which involve the Jacobian for the case of curves, and the Picard variety as well as the torsion part of the Neron-Severi group in higher dimension.

We shall now reprove for global fields the weak part of the Mordell-Weil theorem, i. e. Theorem 3 below.

PROPOSITION 10. *Let A be an abelian variety defined over a field k. Let m be prime to the characteristic of k and let $K = k(1/m \cdot A_k)$. Then $(A_k \colon mA_k)$ is finite if and only if $[K \colon k]$ is finite.*

Proof. It is trivial that if $(A_k \colon mA_k)$ is finite, then $[K \colon k]$ is finite. Conversely, consider the exact sequence

$$0 \to A_m \to A_K \to mA_K \to 0$$

Let $G = G(K/k)$. We have the cohomology sequence

$$0 \to A_m \cap A_k \to A_k \to mA_K \cap A_k \to H^1(G, A_m).$$

By assumption, $mA_K \cap A_k = A_k$, and thus we get the injection

$$0 \to A_k/mA_k \to H^1(G, A_m)$$

which shows that A_k/mA_k is finite.

COROLLARY. *Let A be an abelian variety defined over a field k, and let m be a natural number prime to the characteristic of k. Let L be a finite extension of k. If A_L/mA_L is finite then so is also A_k/mA_k.*

Proof. By the proposition, $L(1/m \cdot A_L)$ is finite over L. This implies a fortiori that $k(1/m \cdot A_k)$ is finite over k. Using the proposition once more, we get what we want.

THEOREM 3. *Let A be an abelian variety defined over an m-global field k. Then A_k/mA_k is finite.*

Proof. By the corollary, we may assume that $A_m \subset A_k$. Let $K = k(1/m \cdot A_k)$. By Proposition 9, we know that K/k is unramified at every prime $\mathfrak{p}$ not dividing m at which A has a non-degenerate reduction. From the definition of m-global, it follows that K is finite over k because it is abelian of exponent m over k. We now apply Proposition 10, to conclude the proof.

If K is a finite Galois extension of k, and if A is an abelian variety defined over k such that its group of rational points A_K in K is finitely generated (i. e. satisfies the strong Mordell-Weil theorem), then obviously $H^r(K/k, A)$ is finite for $r > 0$. However, Theorem 3 will suffice to prove the analogous result for m-global fields. For use in the statement of our next theorem, we recall that the m-primary part of an abelian group consists of those elements whose period divides a power of m.

THEOREM 4. *Let A be an abelian variety defined over an m-global* *field k. If K/k is a finite Galois extension, then the m-primary part of the group $H^r(K/k, A)$ is finite for each $r > 0$.*

Proof. This is an immediate consequence of the following general cohomological fact.

LEMMA. *Let G be a finite group and X a G-module such that X/mX and X_m are finite. Then the m-primary part of $H^r(G, X)$ is finite for each $r > 0$.*

Proof. Since $H^r(G, X)$ is a torsion group of bounded exponent $(G\colon 1)$, it is enough to prove $H^r(G, X)_m$ finite. The map $m\colon X \to X$ can be written as a product $m = g \circ h$ of the maps g and h in the exact sequences

$$0 \to X_m \to X \xrightarrow{h} mX \to 0$$

$$0 \to mX \xrightarrow{g} X \to X/mX \to 0.$$

For the induced cohomology maps in dimension r, we have $m_* = g_* h_*$. From the exact cohomology sequences derived from our two exact sequences, we see that the kernels of h_* and g_* are finite, being homomorphic images of $H^r(G, X_m)$ and $H^{r-1}(G, X/mX)$ respectively. Consequently, the kernel of m_* is finite, which is what we wanted to prove.

If A is an abelian variety defined over an m-global field k, we say that an element $\alpha \in H^1(k, A)$ *splits at a prime* $\mathfrak{p}$ of k if α is in the kernel of the canonical map $H^1(k, A) \to H^1(k_{\mathfrak{p}}, A)$, where $k_{\mathfrak{p}}$ denotes the completion of k at $\mathfrak{p}$. In other words, α splits at $\mathfrak{p}$ if the corresponding homogeneous space has a rational point in $k_{\mathfrak{p}}$.

Selmer [11] has given examples of principal homogeneous spaces for abelian varieties of dimension 1 over the rational number field $\boldsymbol{Q}$ which split at all primes p but do not split in $\boldsymbol{Q}$. The elliptic curve $3X^3 + 4Y^3 + 5Z^3 = 0$ is such a space over its Jacobian. On the other hand, we can show that the number of such spaces with given period is finite. More precisely, let us denote by $H^1(k, A, S)$ the subgroup of $H^1(k, A)$ consisting of the elements which split at all primes outside a finite set S. We have

THEOREM 5. *Let A be an abelian variety defined over an m-global field k. Then $H^1(k, A, S)_m$ is finite.*

Proof. Without loss of generality, we may assume $A_m \subset A_k$. Indeed, the restriction of $H^1(k, A)$ to $H^1(K, A)$, where $K = k(A_m)$, has finite kernel by Theorem 4, and a fortiori that of $H^1(k, A, S)_m$ to $H^1(K, A, S)_m$. Furthermore, we may enlarge S until it contains all primes $\mathfrak{p}$ dividing m

and all primes $\mathfrak{p}$ where A does not have a non-degenerate reduction. Now for $\mathfrak{p} \notin S$, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_k/mA_k \arrow[r] \arrow[d] & \mathrm{Hom}(G_k, A_m) \arrow[r] \arrow[d] & H^1(k, A)_m \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_\mathfrak{p}/mA_\mathfrak{p} \arrow[r] & \mathrm{Hom}(G_\mathfrak{p}, A_m) \arrow[r] & H^1(k_\mathfrak{p}, A)_m \arrow[r] & 0.
\end{tikzcd}$$

Here we have abbreviated by $A_\mathfrak{p}$ the group $A_{k_\mathfrak{p}}$ and by $G_\mathfrak{p}$ the decomposition group $G_{k_\mathfrak{p}}$ which we may view as a subgroup of G_k, uniquely determined up to a conjugation. The horizontal arrows are the exact Kummer sequences and the vertical arrows are the canonical maps, the middle one therefore denoting simply the operation of restricting to $G_\mathfrak{p}$ a homomorphism of G_k. What we shall actually prove is that the inverse image of $H^1(k, A, S)_m$ in $\mathrm{Hom}(G_k, A_m)$ is finite. To this effect, it will be enough to show that if $\chi\colon G_k \to A_m$ is a homomorphism whose cohomology class in $H^1(k, A)$ splits outside S, then the abelian extension K_χ/k of exponent m which is cut out by the kernel of χ is unramified outside S. By the commutativity of the right square of the above diagram we know that the restriction of χ to G_p is of the form $\chi(\sigma) = (\sigma - 1)(1/m \cdot a)$ for some $a \in A_\mathfrak{p}$. Thus we have $K_\chi \subset k_\mathfrak{p}(1/m \cdot a)$, and, by Proposition 9, it follows that K_χ is unramified at $\mathfrak{p}$. This completes the proof of Theorem 5.

It is natural to raise the question whether, given an element of $H^1(k_\mathfrak{p}, A)$, there exists an element of $H^1(k, A)$ which restricts to it. We can prove this in a special case.

THEOREM 6. *Let k be any field with a discrete valuation $\mathfrak{p}$ and let $k_\mathfrak{p}$ be its completion. Let m be prime to the characteristic of k and assume that the group of m-th roots of unity Ω_m lies in k. Let A be an abelian variety defined over k such that $A_m \subset A_k$. Then given $\alpha_\mathfrak{p} \in H^1(k_\mathfrak{p}, A)_m$, there exists an element $\alpha \in H^1(k, A)_m$ whose canonical image in $H^1(k_\mathfrak{p}, A)$ is $\alpha_\mathfrak{p}$.*

Proof. We use the Kummer sequence again, and the exact commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(G_k, A_m) \arrow[r] \arrow[d] & H^1(k, A)_m \arrow[r] \arrow[d] & 0 \\
\mathrm{Hom}(G_\mathfrak{p}, A_m) \arrow[r] & H^1(k_\mathfrak{p}, A)_m \arrow[r] & 0.
\end{tikzcd}$$

We are trying to prove that the right hand vertical arrow is surjective. To do so, it is enough to prove the left hand vertical arrow is surjective. Since

A_m is isomorphic as an abstract group to the direct sum of $2r$ copies of Ω_m $(r = \dim A)$, we have

$$\mathrm{Hom}(G, A_m) \approx (\mathrm{Hom}(G, \Omega_m))^{2r},$$

and, consequently, it is enough if we show the surjectivity of

$$\mathrm{Hom}(G_k, \Omega_m) \to \mathrm{Hom}(G_{\mathfrak{p}}, \Omega_m).$$

Recall now that Hom means here continuous homomorphisms, so that by the usual Kummer duality, we have $\mathrm{Hom}(G_k, \Omega_m) \approx k^*/(k^*)^m$, and similarly for $k_{\mathfrak{p}}$. Thus, we must simply show the surjectivity of $k^*/(k^*)^m \to k_{\mathfrak{p}}^*/(k_{\mathfrak{p}}^*)^m$. This is now obvious since $(k_{\mathfrak{p}}^*)^m$ is an open subgroup of $k_{\mathfrak{p}}^*$, m being prime to the characteristic.

Remark. Under the same hypotheses as in the theorem, one can deal with a finite number of discrete valuations, and use the approximation theorem to show that there is an α restricting simultaneously to a finite number of given $\alpha_{\mathfrak{p}_i}$.

In analogy with Grunwald's theorem in class field theory, one may conjecture that if k is an algebraic number field and $\mathfrak{p}$ a given prime, then given $\alpha_{\mathfrak{p}} \in H^1(k_{\mathfrak{p}}, A)$, there exists $\alpha \in H^1(k, A)$ restricting to $\alpha_{\mathfrak{p}}$.

Finally, we prove a result indicating that $H^1(k, A)$ is usually a large group when k is a global field.

THEOREM 7. *Let m be a natural number and let k be a field with an infinite number of abelian extensions of exponent exactly m. Let A be an abelian variety defined over k such that* (1) *A_k/mA_k is finite and* (2) *A_k contains at least one element a of exact period m. Then $H^1(k, A)$ contains an infinite number of elements of period m, and, in fact, an infinite number such that the corresponding homogeneous spaces have index m as well as period m.*

Proof. Let $L = k(1/m \cdot A_k)$. Since we have assumed A_k/mA_k finite, L is a finite extension of k. Consequently, by our hypothesis about the existence of abelian extensions of exponent m, there exists a Galois extension K of k linearly disjoint from L whose group $G = G(K/k)$ is the direct product of an arbitrarily large number of cyclic groups of order m. For each homomorphism χ of G into the cyclic group $\langle a \rangle$ of order m generated by a, let $\alpha_\chi \in H^1(K/k, A) \subset H^1(k, A)$ denote the cohomology class of the 1-cocycle $\sigma \to \chi(\sigma)$. We claim that the map $\chi \to \alpha_\chi$ is an injection. Indeed, if $\chi(\sigma) = (\sigma - 1)b$, $b \in A_K$, $\sigma \in G$, then $m\chi(\sigma) = (\sigma - 1)mb = 0$ for all σ; hence $mb \in A_k$. Since K is disjoint from L, it follows that $b \in A_k$ and $\chi = 0$.

Thus, $H^1(k,A)$ contains a subgroup isomorphic to $\mathrm{Hom}(G,\langle a\rangle)$, that is, to the direct product of arbitrarily many cyclic groups of order m. Moreover, for each element of this subgroup, the corresponding homogeneous space has index $=$ period. This follows from the Corollary of Proposition 5, § 2 because, since $\langle a\rangle$ is cyclic, the index in G of the kernel of the homomorphism $\chi\colon G\rightarrow\langle a\rangle$ is equal to the period of χ, and the subfield of K cut out by this kernel splits α.

PARIS.

REFERENCES.

[1] A. Albert, "On primary normal division algebras of degree 8," *Bulletin of the American Mathematical Society*, vol. 39 (1933), pp. 265-272.

[2] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1956.

[3] F. Chatelet, "Méthode Galoisienne et courbes de genre 1," *Annales de l'Universite de Lyon*, Section A., t. 89 (1946), pp. 40-49.

[4] ———, "Variations sur un thème de Poincaré," *Annales de l'Ecole Normale superieure*, vol. 59 (1944), pp. 249-300.

[5] W. L. Chow and S. Lang, "On the birational equivalence of curves under specialization," *American Journal of Mathematics*, vol. 79, No. 3 (1957), pp. 649-652.

[6] J. Igusa, "Fibre systems of Jacobian varieties, II," *American Journal of Mathematics*, vol. 78 (1956), pp. 745-760.

[7] S. Lang, "Algebraic groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[8] E. Lutz, "Sur l'équation $y^2=x^3-Ax-B$ dans les corps p-adiques," *Journal für die reine und angewandte Mathematik*, Bd. 177 (1937), pp. 238-247.

[9] A. Mattuck, "Abelian varieties over p-adic ground fields," *Annals of Mathematics*, Series 2, vol. 62 (1955), pp. 92-119.

[10] P. Roquette, "Über das Hassesche Klassenkorper-Zerlegungesetz," *Journal für die reine und angewandte Mathematik*, Bd. 197 (1957), pp. 49-67.

[11] E. Selmer, "The diophantine equation $ax^3+by^3+cz^3=0$," *Acta Mathematika*, vol. 85 (1951), pp. 203-362.

[12] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[13] A. Weil, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955), pp. 493-512.

[14] ———, "The field of definition of a variety," *American Journal of Mathematics*, vol. 78 (1956), pp. 509-524.

EXTENSIONS OF VECTOR GROUPS BY ABELIAN VARIETIES.*[1]

By MAXWELL ROSENLICHT.

This paper gives, among other things, the detailed proofs of a number of results previously announced by the author (cf. [10, § 5] and [11]; also [7, § 2] and [8]). The point of departure was the problem of finding a good geometric theory for the simple differentials of second kind on an algebraic variety. Such a theory, at least in the case of characteristic zero, is essentially contained (via the Albanese map) in the corresponding theory for abelian varieties, and it quickly became apparent that the proper object of study is the set of all algebraic group extensions of direct products of additive groups over a given abelian variety. The set of equivalence classes of extensions of the one-dimensional additive group by a given abelian variety A is naturally endowed with the structure of a vector space (over the universal domain), and the main results say that this vector space has the same dimension as A (Th. 3) and is naturally isomorphic to the cohomology space $H^1(A, \mathfrak{O}_A)$, $\mathfrak{O}_A$ being the sheaf of local rings on A (Th. 1). (A form of the first result that concerns the possible direct product decompositions of group extensions over A is misstated in our previous papers; this hinges on the fact that a product of additive groups may be susceptible of more than one vector space structure. The correct statement is in Prop. 11.) We leave aside the question of differentials of the second kind, concentrating on the matter of group extensions, but the relation between the two subjects can be gathered from the characteristic zero part of the proof of Prop. 11 (see Lemma 3 and the remark following the Prop.). This last mentioned part is the only place where our methods are not purely algebraic and where there is an essential difference between the case of characteristic zero and $p \neq 0$. A purely algebraic proof of the point in question could have been given, but would have been long. (Such a proof of the dimensionality of the space of extensions can be found in [1], a paper which is mostly restricted to characteristic zero and is in large part an algebraization of [8]; Barsotti has also published a proof of the same fact for characteristic $p \neq 0$ that is based on the infinitesimal

---

* Received January 21, 1958.

[1] This research was supported in large part by the U. S. Air Force through the Air Force Office of Scientific Research, part of the Air Research and Development Command under contract No. AF 18(600)-1571.

analysis of inseparable isogenies [2].) Some additional information on differentials of second kind can be found in an appendix where we prove some facts on the invariant differential forms on generalized jacobian varieties (stated without proof in [7] and [11]) which will have future utility.

A correspondence with J-P. Serre resulted in the simplification of some of the author's original ideas, as well as in a number of corrections. Serre will publish shortly some of his own contributions to the theory, notably the fact that the cohomology ring of an abelian variety (sheaf of local rings) is an exterior algebra. Part of a recent course of his ([16], to be published eventually in book form) was devoted to the present theory, and many sections here are very close to his notes (although there is a quite different proof of our Th. 1, whose full generality was discovered independently). We are especially indebted to Serre for certain of the useful trivialities on group extensions (beginning of our § 2) and for the exact sequences of Propositions 6 and 7.

1. Products of additive groups. The results of this section are probably well-known in the correct circles, although mainly unpublished. We have added something in the way of rationality statements and simplified proofs. The basic reference to linear algebraic groups is [3].

By a *vector group* we mean a commutative algebraic group G together with a regular operation of the multiplicative group G_m on G with the property that there exists a biregular birational correspondence between G and the ordinary affine space of the same dimension which is such that the group structure on G and the operation of G_m on G are those induced by the usual vector space structure on the affine space. It is clear what is meant by a *linear function on G, vector subgroup of G, linear homomorphism* (from one vector group into another), etc. If k is a field of definition for G as an algebraic group and for the operation of G_m on G, we say that k is a *field of definition for the vector group G.* Such being the case, any linear function on G is a linear combination with constant coefficients of linear functions that are defined over k, and if $n = \dim G$ it follows that functions $x_1, \cdots, x_n$ on G can be found such that the map $g \rightarrow (x_1(g), \cdots, x_n(g))$ is a biregular birational correspondence, defined over k, between G and the n-dimensional affine space and the vector group structure on G is given by the usual rules $x_i(g_1 + g_2) = x_i(g_1) + x_i(g_2)$, $x_i(cg) = cx_i(g)$; such functions $x_1, \cdots, x_n$ will be called *linear coordinate functions on G.*

The additive group G_a consists of the affine line with the composition law $(x_1)(x_2) = (x_1 + x_2)$. The additive parameter x on G_a is characterized to within multiplication by nonzero constants as an everywhere finite rational function on G_a that vanishes to first order at the identity 0 and has no other zero. Thus G_a can be considered, in a well-defined way, to be a vector group. The algebraic group $(G_a)^n$ ($= G_a \times G_a \times \cdots \times G_a$, n times) can be endowed with the structure of a vector group (namely that induced by the natural vector group structure of each direct factor), but if $n > 1$ the group $(G_a)^n$ may possess various distinct vector group structures consistent with its underlying algebraic group structure. Functions $x_1, \cdots, x_n$ that are linear coordinate functions on $(G_a)^n$ with respect to one of its admissible vector group structures will be called *additive coordinate functions on* $(G_a)^n$.

Suppose we have a rational homomorphism $G_a \rightarrow G_a$. Fixing a coordinate function on G_a, this homomorphism is given by $x \rightarrow f(x)$, where $f(x)$ is a polynomial satisfying $f(x_1 + x_2) = f(x_1) + f(x_2)$. One deduces immediately that we can write

$$f(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_m x^{p^m},$$

where m is some positive integer, $a_0, \cdots, a_m$ are constants, and p is the field characteristic, if this differs from zero; in the case of characteristic zero, $f(x) = ax$, with a constant. In either case we call a function $f(x)$ of this form a *p-polynomial in x* (a term originally due to O. Ore), and we note that, conversely, any p-polynomial in x produces a rational endomorphism $G_a \rightarrow G_a$. As a consequence, if $\tau : (G_a)^n \rightarrow (G_a)^m$ is a rational homomorphism and $(x_1, \cdots, x_n)$, $(y_1, \cdots, y_m)$ are additive coordinate functions on the two groups, we have

$$y_i(\tau x) = f_{i1}(x_1) + \cdots + f_{in}(x_n), \qquad i = 1, \cdots, m,$$

where each f_{ij} is a p-polynomial in one variable. Such a function $f_{i1}(x_1) + \cdots + f_{in}(x_n)$ we call a *p-polynomial in $x_1, \cdots, x_n$*, and we note that, conversely, any m such p-polynomials in $x_1, \cdots, x_n$ give a rational homomorphism $\tau : (G_a)^n \rightarrow (G_a)^m$. In characteristic zero, a p-polynomial is a homogeneous linear function. All this implies that if $x_1, \cdots, x_n$ are additive coordinate functions on $(G_a)^n$ and $y_1, \cdots, y_n$ are rational functions on the same group, then this latter set is also a set of additive coordinate functions on $(G_a)^n$ if and only if each of the y's is a p-polynomial in the various x's, and conversely, each of the x's is a p-polynomial in the various y's. This enables us to find all possible admissible vector group structures on $(G_a)^n$, and it is clear that if the characteristic is $p \neq 0$ and $n > 1$, an infinite number of such vector group structures is possible, whereas in the case of characteristic zero the vector group structure is unique.

PROPOSITION 1. *Let H be a connected algebraic subgroup of $(G_a)^n$, k a field of definition for the solvability of H* (cf. [12, § 4]). *Then $(G_a)^n$ possesses an admissible vector group structure, also defined over k, with respect to which H is a vector subgroup.*

This is trivial if $\dim H = 0$, so suppose $\dim H > 0$. Then there exists an algebraic subgroup Γ of H which is biregularly isomorphic to G_a over k. Letting $x \in k(\Gamma)$ be an additive parameter on Γ and $x_1, \cdots, x_n$ be additive coordinates on $(G_a)^n$, each of the n functions $x_i(x)$ is a p-polynomial in x with coefficients in k, and not all $x_i(x)$ are zero. Consider coordinate changes on $(G_a)^n$ which interchange the coordinates $x_1, \cdots, x_n$, or which replace $x_1, \cdots, x_n$ by $x_1, x_2', \cdots, x_n'$, where each x_i' $(i = 2, \cdots, n)$ is the sum of x_i and a p-polynomial in $k[x_1]$. By interchanging $x_1, \cdots, x_n$, we can guarantee that the minimal degree of the nonzero $x_i(x)$'s is attained for $i = 1$, then by a coordinate change of the second type we can arrange that each nonzero $x_i(x)$, for $i > 1$, has degree less than that of $x_1(x)$. Hence, by repeated changes of this sort, we can insure that $x_i(x) = 0$ for $i = 2, \cdots, n$, which completes the proof if $\dim H = 1$. If $\dim H > 1$, we continue the same reasoning on $(G_a)^n/\Gamma$, etc.

The following proposition shows, among other things, that any algebraic group that is isogenous to a direct products of G_a's is also of this type, as is any homomorphic image of such a group. If such a group has k as a field of definition for its solvability, then it is biregularly isomorphic to a direct product of G_a's over k. Note that by [14, Prop. 5, Cor. 2], a perfect field of definition of such a group is always a field of definition for its solvability.

PROPOSITION 2. *Let the commutative algebraic group H be defined over k. If the characteristic is $p \neq 0$, suppose that $p \cdot h = 0$ for each $h \in H$, while if the characteristic is zero, suppose merely that H is linear and each of its elements is unipotent. Then there exists a biregular isomorphism, defined over k, from H into a direct product of G_a's.*

In the case of characteristic $p \neq 0$, the condition $p \cdot h = 0$ shows that no homomorphic image of H_0 is an abelian variety, so that here too H is linear and each of its elements is unipotent. Thus, in any case, we can suppose that H is a group of square matrices, each of which is of the form $I + \mu$, where I denotes the identity matrix, μ a nilpotent matrix (of order p if the characteristic is $p \neq 0$), and "$+$" ordinary addition of matrices, and where any two such matrices μ commute. Denoting by M the linear space spanned by all matrices μ such that $I + \mu \in H$, we get that M is defined over k and is a commutative algebra under matrix multiplication each of whose elements is nilpotent (of order p if the characteristic is $p \neq 0$). The set G consisting of all matrices $I + m$, with $m \in M$, is a commutative algebraic group, defined over k and containing H. We prove that G is biregularly isomorphic over k to $(G_a)^n$, where $n = \dim M$. For this, note that $M \supset M^2 \supset M^3 \supset \cdots$, all these inclusions being proper until 0 is reached. Choose a basis $m_1, \cdots, m_n$ of M, each m_i being rational over k, such that for each $i = 1, \cdots, n-1$ the elements $m_{i+1}, \cdots, m_n$ span a subspace of M that is an M-submodule containing m_i^2. For any quantities $x_1, \cdots, x_n$, consider the expression $(\exp x_1 m_1) \cdots (\exp x_n m_n)$ (where in characteristic $p \neq 0$, exp denotes the first p terms of the exponential series); this clearly gives us a rational homomorphism defined over k from $(G_a)^n$ into G. It is easy to verify that

$$k((\exp x_1 m_1) \cdots (\exp x_n m_n)) = k(x_1, \cdots, x_n),$$

which completes the proof.

The remainder of this section is devoted to finding canonical forms for homomorphisms of products of G_a's.

LEMMA. *Let k be a field, $x_1, \cdots, x_n$ quantities that are algebraically independent over k, let $\nu_1, \cdots, \nu_n$ be integers > 0, and let $y_1, \cdots, y_n$ be elements of $k[x]$ such that $y_i - x_i^{\nu_i}$ is an element of $k[x]$ of total degree less than ν_i, $i = 1, \cdots, n$. Then $k(x)$ is an algebraic extension of $k(y)$ of degree $\nu_1 \nu_2 \cdots \nu_n$.*

We shall in fact prove more, namely that $k[x]$ is a free module over $k[y]$ having as generators the various quantities $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where $0 \leqq \alpha_i < \nu_i$, $i = 1, \cdots, n$. Let M be the $k[y]$-module generated by these quantities. Any power product of $x_1, \cdots, x_n$ can be written in the form $x_1^{\beta_1 \nu_1 + \alpha_1} \cdots x_n^{\beta_n \nu_n + \alpha_n}$, with $\beta_1, \cdots, \beta_n$ integers $\geqq 0$ and $\alpha_1, \cdots, \alpha_n$ as above, and this monomial differs from $y_1^{\beta_1} \cdots y_n^{\beta_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by an element of $k[x]$ of total degree $< \sum_{i=1}^{n} (\beta_i \nu_i + \alpha_i)$; thus each element of $k[x]$ can be written as an element of M plus another element of $k[x]$ of smaller total degree, and we deduce that $k[x] = M$. Finally, we must show that an expression

$$\sum_{\substack{\beta_1, \cdots, \beta_n \geqq 0 \\ 0 \leqq \alpha_i < \nu_i}} c_{\beta_1, \cdots, \beta_n, \alpha_1, \cdots, \alpha_n} y_1^{\beta_1} \cdots y_n^{\beta_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

(where each $c_{\beta, \alpha} \in k$ and not all are zero) cannot vanish. If Γ is the subset of $\{(\beta, \alpha)\}$ consisting of those $2n$-tuples (β, α) for which $c_{\beta, \alpha} \neq 0$ and

$\sum_{i=1}^{n}(\beta_i\nu_i + \alpha_i)$ is maximal, then the above expression is congruent modulo terms of lower total degree to

$$\sum_{(\beta,\alpha)\in\Gamma} c_{\beta,\alpha}x_1^{\beta_1\nu_1+\alpha_1}\cdots x_n^{\beta_n\nu_n+\alpha_n}.$$

But the various terms in this last sum are distinct, so our original sum is $\neq 0$.

PROPOSITION 3. *Let H be a vector group of dimension n, $\tau\colon H \rightarrow (G_a)^m$ a surjective rational homomorphism (of the additive structure of H only), all defined over the perfect field k of characteristic $p \neq 0$. Then there exist linear coordinate functions $x_1,\cdots,x_n$ on H and additive coordinate functions $y_1,\cdots,y_m$ on $(G_a)^m$, all defined over k, such that τ is given by*

$$y_i = x_i^{p^{\nu_i}} + (\textit{a } p\textit{-polynomial in } k[x] \textit{ of degree} < p^{\nu_i}), \qquad i = 1,\cdots,m.$$

Furthermore, if τ is an isogeny, its degree is $p^{\nu_1}\cdots p^{\nu_n}$.

First pick any linear coordinate functions $x_1,\cdots,x_n$ on H and additive coordinate functions $y_1,\cdots,y_m$ on $(G_2)^m$, all defined over k, and write

$$y_i = u_i^{p^{\nu_i}} + (\text{a } p\text{-polynomial in } k[x] \text{ of degree} < p^{\nu_i}), \qquad i = 1,\cdots,m,$$

where $u_1,\cdots,u_m$ are each nonzero linear combinations of $x_1,\cdots,x_n$ with coefficients in k. Keep $x_1,\cdots,x_n$ fixed and alter the additive coordinate functions $y_1,\cdots,y_m$ on $(G_a)^m$ so that $(\nu_1,\nu_2,\cdots,\nu_m)$ is minimal in the lexicographical ordering, i.e., $y_1,\cdots,y_m$ are so chosen that ν_1 is minimal, ν_2 is minimal for this fixed ν_1, etc. Then $0 \leqq \nu_1 \leqq \cdots \leqq \nu_m$. If for some $i = 2,\cdots,m$ we had u_i linearly dependent on $u_1,\cdots,u_{i-1}$, then by subtracting from y_i a suitable p-polynomial in $y_1,\cdots,y_{i-1}$, we could get new additive coordinate functions on $(G_a)^m$ giving rise to the same $\nu_1,\cdots,\nu_{i-1}$ and a strictly smaller ν_i; thus $u_1,\cdots,u_m$ are linearly independent. Hence we may alter our x's so that $x_1 = u_1,\cdots,x_m = u_m$; all is now proved, except for the last statement, which comes from the lemma.

PROPOSITION 4. *Let $\tau\colon (G_a)^n \rightarrow (G_a)^m$ be a surjective rational homomorphism, defined over the infinite perfect field k of characteristic $p \neq 0$. Then there exist additive coordinate functions $x_1,\cdots,x_n$ on $(G_a)^n$ and $y_1,\cdots,y_m$ on $(G_a)^m$, all defined over k, such that τ is given by*

$$y_1 = x_1^{p^{\alpha_1}},\cdots,y_{m-1} = x_{m-1}^{p^{\alpha_{m-1}}}, \quad y_m = x_m^{p^{\alpha_m}} + \sum_{s>0} c_s x_m^{p^{\alpha_m+s}},$$

where $0 \leqq \alpha_1 \leqq \cdots \leqq \alpha_m$ are integers and $c_1, c_2,\cdots \in k$.

Using Prop. 1, additive coordinate functions for $(G_a)^n$, all defined over k, can be found such that the component of the identity of the kernel of τ is got by setting certain of these coordinate functions equal to zero. It follows that we can assume that τ is an isogeny, i. e., that its kernel is finite. (This implies, in particular, that $n = m$, but we shall maintain use of the two letters to distinguish the two groups involved.) The result is clear if $n \leqq 1$, so assume $n > 1$ and use induction. Take any additive coordinate functions on the two groups, say $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ respectively, all defined over k. Let α_1 be the greatest integer α such that $k[y] \subset (k[x])^{p^\alpha}$; since $k[x]$ is the ring of all everywhere finite rational functions on $(G_a)^n$ that are defined over k, and similarly for $k[y]$, the integer α_1 is independent of the choice of the x's and y's. When we express the y's as p-polynomials in the x's, all powers are at least to the p^{α_1}-th, and this power actually occurs. Choose elements $a_1, \cdots, a_n \in k$, not all zero, so that the one-parameter subgroup Γ of $(G_a)^n$ given by $x_1 = a_1 t, \cdots, x_n = a_n t$ meets the kernel of τ only at the identity and so that the degree of the map $\tau\colon \Gamma \rightarrow (G_a)^m$ is p^{α_1} (and no higher). By a linear change of the coordinates $x_1, \cdots, x_n$ we can assume that $a_1 = 1, a_2 = \cdots = a_n = 0$, and by a suitable change of $y_1, \cdots, y_m$, we can suppose that $\tau\Gamma$ is the subgroup $y_2 = \cdots = y_m = 0$ of $(G_a)^m$. Then $y_2, \cdots, y_m$ are independent of x_1 and y_1 is a linear combination of $x_1^{p^{\alpha_1}}$ and powers of $x_2, \cdots, x_n$ at least as high. Thus $y_1 = (x_1')^{p^{\alpha_1}}$, where x_1' differs from a nonzero constant multiple of x_1 by a p-polynomial in $x_2, \cdots, x_n$. Altering x_1 to x_1' we get $y_1 = x_1^{p^{\alpha_1}}$ and $y_2, \cdots, y_m \in k[x_2, \cdots, x_n]$, so that our induction assumption is applicable to the homomorphism $(G_a)^{n-1} \rightarrow (G_a)^{m-1}$ given by $(x_2, \cdots, x_n) \rightarrow (y_2, \cdots, y_m)$. We remark that a standard argument (considering $[k(y, x^{p^\nu}) : k(x^{p^\nu})]_i$, for various ν) shows the unicity of $\alpha_1, \cdots, \alpha_m$, and that we can dispense with the condition that k be infinite if the kernel of τ is connected.

2. Algebraic group extensions. Let G_1, G_2, G_3 be algebraic groups. A sequence of homomorphisms

$$G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3$$

will be called *exact* if, as usual, $\operatorname{Im} \phi_1 = \operatorname{Ker} \phi_2$ and, in addition, ϕ_1 and ϕ_2 are separable rational homomorphisms; similarly for longer sequences. If the above sequence is exact, then the corresponding sequence of Lie algebra homomorphisms

$$\mathfrak{g}_1 \rightarrow \mathfrak{g}_2 \rightarrow \mathfrak{g}_3$$

is also exact (e. g., cf. [13]). Conversely, if we are given a sequence of rational homomorphisms of algebraic groups that is exact in the purely group-theoretic sense (i. e. we drop the condition that the various homomorphisms be separable) then we get a corresponding sequence of Lie algebra homomorphisms, and if the latter sequence is exact, so is the sequence of algebraic groups. (This amounts to showing that if $\psi\colon G \to G'$ is a purely inseparable isogeny of algebraic groups such that the corresponding Lie algebra map is an isomorphism, then ψ itself is a biregular isomorphism. This follows from the fact that we have an induced isomorphism between the spaces of local differentials at the identities of G and G' respectively, so ψ is separable.)

Let H and A be algebraic groups. By an *extension of H by A* (or *over A*) is meant an algebraic group G together with an exact sequence

$$0 \to H \to G \to A \to 0,$$

0 being the group with one element. Here H can be identified with a normal algebraic subgroup of G and A with G/H; when no confusion is possible, we shall often call G itself an extension of H by A. If the various groups and homomorphisms are defined over a field k, we say that the extension is *defined over k*. Another extension G' of H by A is called *equivalent* to the above extension if there exists a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\psi"'] & A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H \arrow[r] & G' \arrow[r] & A \arrow[r] & 0,
\end{tikzcd}$$

where ψ is a rational homomorphism and each of the two outside vertical maps is the identity; in this case, ψ is automatically a biregular isomorphism (for it is bijective, hence a purely inseparable isogeny, and the Lie algebra diagram associated with the above is commutative, so that ψ induces a Lie algebra isomorphism, hence is separable). The extension G of H by A is called *inessential* if, τ being the natural homomorphism from G to A, there exists a rational homomorphism $\phi\colon A \to G$ such that $\tau\phi =$ identity. In this case, ϕ must be birational, so that A may be identified with an algebraic subgroup of G. This being done, we conclude from $G = HA$, $H \cap A = 0$, the separability of the homomorphism $A \to G/H$ and [12, Prop. 2] that the map $H \times A \to G$ defined by $h \times a \to ha$ is biregular.

If H and A are commutative algebraic groups, we shall denote by $\mathrm{Ext}(A, H)$ the set of equivalence classes of commutative extensions of H by A. (Much of what follows will go through under more general circumstances, namely that H be commutative and the restrictions of the inner automorphisms of the extension group to H be given by a specific operation of A as a group of rational automorphisms of H. In any case, we are mainly interested in what happens when H is connected and commutative and A is an abelian variety, and here an extension group is always commutative [12, Th. 13, Cor. 2]; thus all algebraic groups in the remainder of § 2 will be assumed commutative.) We proceed to outline the functorial properties of $\operatorname{Ext}(A,H)$, leaving most of the details of proof to the reader. These details are all easy, except for the occasional question of separability, which is always to be handled by [12, Prop. 1]; at any rate, the next proposition is almost trivial from the point of view of factor systems (see below), which will be applicable in all special cases we later consider.

If $\phi\colon A'\to A$ is a rational homomorphism and $G\in\operatorname{Ext}(A,H)$, let G' be the subgroup of $A'\times G$ consisting of all $a'\times g$ such that a' and g have the same image in A. If we map H into G' by $h\to 0\times h$, we get that G' is an extension of H by A'. Hence we have a map $\phi^*\colon \operatorname{Ext}(A,H)\to\operatorname{Ext}(A',H)$. If $\phi=\text{identity}$, then $\phi^*=\text{identity}$, and if $\phi'\colon A''\to A'$, then $(\phi\phi')^*=\phi'^*\phi^*$.

If $\psi\colon H\to H'$ is a rational homomorphism and $G\in\operatorname{Ext}(A,H)$, let $G'=G\times H'/\Delta$, where Δ is the kernel of the homomorphism $H\times H'\to H'$ defined by $h\times h'\to\psi h+h'$. If we map H' into G' by first mapping $h'\in H'$ into $0\times h'\in G\times H'$, G' becomes an extension of H' by A. Hence we have a map $\psi_*\colon\operatorname{Ext}(A,H)\to\operatorname{Ext}(A,H')$. If ψ is the identity, so is ψ_*, and if $\psi'\colon H'\to H''$, then $(\psi'\psi)_*=\psi'_*\psi_*$. In addition, if ϕ is as in the preceding paragraph, the two maps $\phi^*\psi_*, \psi_*\phi^*\colon\operatorname{Ext}(A,H)\to\operatorname{Ext}(A',H')$ are equal.

The method of Baer can now be used to put a composition law on $\operatorname{Ext}(A,H)$: If $G, G'\in\operatorname{Ext}(A,H)$, clearly $G\times G'\in\operatorname{Ext}(A\times A, H\times H)$. Let $\delta\colon A\to A\times A$ be the diagonal map and $\gamma\colon H\times H\to H$ be the group composition and set $G+G'=\delta^*\gamma_*(G\times G')$. This gives a map

$$\operatorname{Ext}(A,H)\times\operatorname{Ext}(A,H)\to\operatorname{Ext}(A,H)$$

which is clearly commutative and admits the trivial extension $A\times H$ as an identity. Associativity is established by reference to the map

$$\operatorname{Ext}(A,H)\times\operatorname{Ext}(A,H)\times\operatorname{Ext}(A,H)\to\operatorname{Ext}(A\times A\times A, H\times H\times H),$$

the diagonal map $A\to A\times A\times A$, and the group composition $H\times H\times H\to H$, while the inverse of an element of $\operatorname{Ext}(A,H)$ is obtained through the automorphism of H that sends h into $-h$. Thus $\operatorname{Ext}(A,H)$ is a commutative group. It is easy to verify that the maps ϕ^*, ψ_* of the two preceding paragraphs are homomorphisms, and equally straightforward, if slightly complicated, to verify that if $\phi_1, \phi_2 \colon A' \to A$ then $(\phi_1 + \phi_2)^* = \phi_1^* + \phi_2^*$ and if $\psi_1, \psi_2 \colon H \to H'$ then $(\psi_1 + \psi_2)_* = \psi_{1*} + \psi_{2*}$. All this can be summarized as follows.

PROPOSITION 5. *If A, H are commutative algebraic groups, then the set* $\operatorname{Ext}(A, H)$, *together with the composition law given above, is a commutative group whose zero element is the trivial extension $A \times H$. With respect to this and the other operations given above,* $\operatorname{Ext}(A, H)$ *is a functor that is contravariant in A, covariant in H, and additive in both A and H.*

COROLLARY.
$$\operatorname{Ext}(A \times A', H) = \operatorname{Ext}(A, H) \times \operatorname{Ext}(A', H),$$
$$\operatorname{Ext}(A, H \times H') = \operatorname{Ext}(A, H) \times \operatorname{Ext}(A, H').$$

We denote by $\operatorname{Hom}(A, H)$ the group of rational homomorphisms from A into H. This clearly satisfies all the functorial properties in Prop. 5.

Now let $0 \to A' \to A \to A'' \to 0$ be an exact sequence of algebraic groups. For any $\tau \in \operatorname{Hom}(A', H)$, consider A to be an element of $\operatorname{Ext}(A'', A')$, and hence get $\tau_* A \in \operatorname{Ext}(A'', H)$. The map $\tau \to \tau_* A$ thus produces a canonical map
$$\operatorname{Hom}(A', H) \to \operatorname{Ext}(A'', H).$$
By Prop. 5, this map is a homomorphism, and is natural in the sense that a rational homomorphism $\psi \colon H \to H'$ produces the usual commutative diagram.

PROPOSITION 6. *Let $0 \to A' \to A \to A'' \to 0$ be an exact sequence of commutative algebraic groups and let H be another commutative algebraic group. Then the sequence of canonical homomorphisms*
$$0 \to \operatorname{Hom}(A'', H) \to \operatorname{Hom}(A, H) \to \operatorname{Hom}(A', H)$$
$$\to \operatorname{Ext}(A'', H) \to \operatorname{Ext}(A, H) \to \operatorname{Ext}(A', H)$$
is exact.

The proof of this is a long but largely mechanical recourse to the various definitions, hence will be omtited. Note that if we have a rational homomorphism $\psi \colon H \to H'$ and write the corresponding exact sequence for H', we get the usual commutative diagram. Each of the groups in the above exact sequence being a module with respect to the ring of rational endomorphisms of H, we see that the various homomorphisms are actually module homomorphisms. Later, we shall be concerned with the case $H = G_a$, and here the homomorphisms are vector space homomorphisms, the scalar field being the universal domain.

Analogously, consider an exact sequence of algebraic groups $0 \to H' \to H$

$\to H'' \to 0$. For any $\tau \in \operatorname{Hom}(A, H'')$, consider H to be an element of $\operatorname{Ext}(H'', H')$ and hence produce $\tau^* H \in \operatorname{Ext}(A, H')$. This map $\tau \to \tau^* H$ gives a canonical map

$$\operatorname{Hom}(A, H'') \to \operatorname{Ext}(A, H').$$

Again by Prop. 5, this map is a homomorphism, natural in the sense that a rational homomorphism $A' \to A$ produces the usual commutative diagram. Although it will not be used in this paper, the following analogue of Prop. 6 is included for completeness. The proof (omitted) is straightforward.

PROPOSITION 7. *Let $0 \to H' \to H \to H'' \to 0$ be an exact sequence of commutative algebraic groups and let A be another commutative algebraic group. Then the sequence of canonical homomorphisms*

$$\begin{aligned} 0 \to \operatorname{Hom}(A, H') \to \operatorname{Hom}(A, H) \to \operatorname{Hom}(A, H'') \\ \to \operatorname{Ext}(A, H') \to \operatorname{Ext}(A, H) \to \operatorname{Ext}(A, H'') \end{aligned}$$

is exact.

Before proceeding, we indicate one consequence of Prop. 6: In most of what follows, we shall be concerned mainly with $\operatorname{Ext}(A, H)$, where A is an abelian variety and H is a connected commutative algebraic group of unipotent matrices. Suppose, more generally, we consider $\operatorname{Ext}(G, H)$, where G is an extension of a torus by an abelian variety, and H is as above. Then we have an exact sequence $0 \to T \to G \to A \to 0$, with T a torus and A an abelian variety, so Prop. 6 gives the exact sequence

$$\operatorname{Hom}(T, H) \to \operatorname{Ext}(A, H) \to \operatorname{Ext}(G, H) \to \operatorname{Ext}(T, H).$$

Here the extreme groups are zero, so $\operatorname{Ext}(G, H)$ is isomorphic to $\operatorname{Ext}(A, H)$.

We now consider briefly the matter of factor systems. If $G \in \operatorname{Ext}(A, H)$ we call a rational map $\sigma : A \to G$ a *cross section* if $\tau\sigma =$ identity, τ being the canonical homomorphism $G \to A$. (By a rational map from one algebraic set, not necessarily irreducible, into another, we mean a law assigning to each component of the first set a rational map from that component into some component of the second algebraic set.) If $\sigma : A \to G$ is a cross section, then the map $A \times H \to G$ sending $a \times h$ into $\sigma a + h$ is birational (in the obvious sense) and we can define a rational map $f_\sigma : A \times A \to H$ by

$$f_\sigma(a_1, a_2) = \sigma a_1 + \sigma a_2 - \sigma(a_1 + a_2).$$

f_σ is a factor system, a *factor system* being a rational map $f : A \times A \to H$ satisfying the equation

$$f(a_1 + a_2, a_3) + f(a_1, a_2) = f(a_1, a_2 + a_3) + f(a_2, a_3),$$

and is symmetric $(f_\sigma(a_1, a_2) = f_\sigma(a_2, a_1))$. Conversely, if $f: A \times A \to H$ is a factor system, we can define a "normal law of composition" on $A \times H$ (obvious extension to reducible sets of the definition of [21]; associativity will correspond to the above equation) by

$$(a_1 \times h_1)(a_2 \times h_2) = (a_1 + a_2, h_1 + h_2 + f(a_1, a_2)),$$

and thus use [21] (with a slight additional argument if A and H are not both connected) to get an algebraic group G that is birationally equivalent to $A \times H$ and has the above composition as group law. If we map H into G by associating to any $h_1 \in H$ the point of G which has the effect on $A \times H$ of moving $a \times h$ into $a \times (h + h_1)$, it is clear that G becomes a central extension of H by A. Commutativity of G will correspond to symmetry of the factor system f, and the factor system f itself can be recovered from the cross section $\sigma: A \to G$ defined by $\sigma(a \times h) = a \times 0$ (a legitimate definition, since the map from $A \times H$ to G is biregular at almost all $a \times h$, and we can use the regular operation of H on both $A \times H$ and G to translate by $-h$). Thus *there is a one-one correspondence between cross sections of elements of* Ext (A, H) *and symmetric factor systems* $f: A \times A \to H$.

If $G \in \operatorname{Ext}(A, H)$ admits the cross section $\sigma: A \to G$, then for any rational map $u: A \to H$ we have a cross section σ' defined by $\sigma' a = \sigma a + ua$; conversely, any cross section $\sigma': A \to G$ is of this form. We get $f_{\sigma'}(a_1, a_2) = f_\sigma(a_1, a_2) + ua_1 + ua_2 - u(a_1 + a_2)$. The factor systems from $A \times A$ to H form a group and those of the form $(a_1, a_2) \to ua_1 + ua_2 - u(a_1 + a_2)$, for some rational map $u: A \to H$, form a subgroup, the group of *trivial factor systems*; the quotient group is the group of *classes of factor systems*. $G \in \operatorname{Ext}(A, H)$ corresponds to the trivial class if and only if there exists a cross section $\sigma: A \to G$ such that $f_\sigma = 0$; thus $\sigma(a_1 + a_2) = \sigma a_1 + \sigma a_2$ and we get $G = A \times H$.

Let $G \in \operatorname{Ext}(A, H)$ admit the cross section $\sigma: A \to G$ and let $\tau: G \to A$ be the canonical homomorphism. Then for any $g \in G$, the map $a \to \sigma(a + \tau g) - g$ is another cross section, which proves, in particular, that a cross section can be found that is defined at any given point of A. Let $\phi: A' \to A$ be a rational homomorphism such that σ is defined along each component of $\phi A'$. If $G' = \phi^* G$ is taken to be a subgroup of $A' \times G$ in the standard way, the map $\sigma': a' \to a' \times \sigma\phi a'$ is a cross section $\sigma': A' \to G'$ and the corresponding factor systems $f_\sigma: A \times A \to H$ and $f_{\sigma'}: A' \times A' \to H$ are related by $f_\sigma(a_1', a_2') = f_\sigma(\phi a_1', \phi a_2')$. Similarly, if we have a rational homomorphism $\psi: H \to H'$ and $G'' = \psi_* G$ is taken to be a quotient of $G \times H'$ in the standard way, the map $\sigma'': A \to G'$ obtained by first mapping a into $\sigma a \times 0$ is a cross section and the factor system $f_{\sigma''}: A \times A \to H'$ is given by $f_{\sigma''}(a_1, a_2) = \psi f_\sigma(a_1, a_2)$. It follows that if $G_1, G_2 \in \operatorname{Ext}(A, H)$ correspond to factor systems f_1, f_2: $A \times A \to H$, then $G_1 + G_2$ corresponds to the factor system $f_1 + f_2$.

PROPOSITION 8. *If A, H are commutative algebraic groups, then the subset of* $\operatorname{Ext}(A, H)$ *consisting of those extensions which admit cross sections is a subgroup, naturally isomorphic to the group of classes of symmetric factor systems from $A \times A$ into H. If H is connected and linear, this subgroup is all of* $\operatorname{Ext}(A, H)$.

Only the last statement remains to be proved, and this follows from the cross section theorem [12, Th. 10]. Note that if A is an abelian variety and H is any connected commutative algebraic group, then *all* factor systems from $A \times A$ to H are symmetric: this comes from the fact that all extensions of H by A are commutative [12, Th. 13, Cor. 2].

3. Principal fiber spaces. For the convenience of the reader, as well as to fix terminology, we recall some concepts familiar in topology. Let H be an algebraic group that operates regularly on an algebraic set B, the operation being indicated by $(h, b) \to bh^{-1}$. B is called a *principal space with respect to H* [22] if the subset of $B \times B$ consisting of all points $b \times bh$ is closed and if there is an everywhere defined rational map θ from this subset into G such that $\theta(b \times bh) = h$. If, in addition, we have another algebraic set V and an everywhere defined surjective rational map $\pi: B \to V$, then B (more properly the triplet $\{B, V, \pi\}$) is called a *principal fiber space over V with group H* if, for any $b \in B$, $\pi^{-1}(\pi b)$ is precisely the orbit bH and if, for any $v \in V$, there exists a rational map $\sigma_v: V \to B$, defined in some neighborhood of v, such that $\pi\sigma_v =$ identity. It is clear what is meant by *isomorphic* principal fiber spaces. If the local cross section $\sigma: V \to B$ is defined on the nonempty open subset U of V, the map $v \times h \to (\sigma v)h$ is clearly a biregular birational map between $U \times H$ and $\pi^{-1}U$. In particular, if V is irreducible, then it is the variety of H-orbits on B, in the sense of [12, Th. 2]. If $\{U_i\}_{i \in I}$ is a finite open covering of V and $\sigma_i: V \to B$ is a cross section that is everywhere defined on U_i then, for $v \in U_i \cap U_j$, we have $(\sigma_i v)h_i = (\sigma_j v)h_j$ if and only if $h_i = (s_{ij}v)h_j$, where $s_{ij}: V \to H$ is the rational map, regular on $U_i \cap U_j$, defined by $s_{ij}v = \theta(\sigma_i v, \sigma_j v)$, and $s_{ij}s_{jk} = s_{ik}$ for all $i, j, k \in I$. Conversely, such an open covering $\{U_i\}_{i \in I}$ of V and regular rational maps $s_{ij}: U_i \cap U_j \to H$ satisfying $s_{ij}s_{jk} = s_{ik}$ for all $i, j, k \in I$ give rise to a principal fiber space $B = \bigcup_{i \in I} U_i \times H$, with the points $v_i \times h_i \in U_i \times H$ and $v_j \times h_j \in U_j \times H$ identified if and only if $v_i = v_j$ and $h_i = (s_{ij}v_i)h_j$,

H operating on B by the rule $(h, v_i \times h_i) \rightarrow v_i \times h_i h^{-1}$ and $\pi(v_i \times h_i) = v_i$ (this is the definition of Weil [19]). As usual, two sets of transition functions $\{s_{ij}\}$ and $\{s'_{ij}\}$ with respect to the same open covering $\{U_i\}_{i \in I}$ of V give rise to isomorphic principal fiber spaces if and only if there exist everywhere regular rational maps $t_i \colon U_i \rightarrow H$ such that $s'_{ij} = t_i^{-1} s_{ij} t_j$, and the isomorphism class of the fiber space got from $\{U_i, s_{ij}\}$ is not altered by passing to a refinement of the covering $\{U_i\}$ and using the same $\{s_{ij}\}$. Thus (cf. [5, pp. 40 ff.]) the classes of principal fiber spaces over V with group H can be identified with the elements of the cohomology set $H^1(V, \mathfrak{H})$, where $\mathfrak{H}$ is the sheaf of germs of locally regular maps from V into H. If H is commutative, we have the usual commutative group structure on $H^1(V, \mathfrak{H})$ [15].

The simplest example of the preceding is the case of an algebraic group G and a connected solvable algebraic subgroup H, H operating on G by the rule $(h, g) \rightarrow gh^{-1}$. If π is the natural map from G to the left coset space G/H, then by [12, Th. 10] there exists a rational cross section $\sigma \colon G/H \rightarrow G$. If σ is regular on the nonempty open subset U of G/H and $g \in G$, then the map $v \rightarrow g^{-1}\sigma(gv)$ is a regular cross section on $g^{-1}U$. The various sets $g^{-1}U$ cover G/H, so G is indeed a principal fiber space.

Let A, H be commutative algebraic groups with H linear and connected. Any extension of H by A is a principal fiber space over A with group H, hence we have a well-defined map $\operatorname{Ext}(A, H) \rightarrow H^1(A, \mathfrak{H})$, $\mathfrak{H}$ being the sheaf of germs of locally regular maps from A into H. If A' is another commutative algebraic group and $\phi \colon A' \rightarrow A$ a rational homomorphism, we have induced homomorphisms $\phi^* \colon \operatorname{Ext}(A, H) \rightarrow \operatorname{Ext}(A', H)$, $\phi^{*\prime} \colon H^1(A, \mathfrak{H}) \rightarrow H^1(A', \mathfrak{H})$, and it is clear from the definition of ϕ^* that the diagram

$$\begin{tikzcd}
\operatorname{Ext}(A, H) \arrow[r] \arrow[d] & H^1(A, \mathfrak{H}) \arrow[d] \\
\operatorname{Ext}(A', H) \arrow[r] & H^1(A', \mathfrak{H})
\end{tikzcd}$$

is commutative. (Cf. the cross section arguments immediately preceding Prop. 8.) Similarly, if H' is another connected commutative linear algebraic group and $\psi \colon H \rightarrow H'$ a rational homomorphism, we have induced homomorphisms $\psi_* \colon \operatorname{Ext}(A, H) \rightarrow \operatorname{Ext}(A, H')$, $\psi_*' \colon H^1(A, \mathfrak{H}) \rightarrow H^1(A, \mathfrak{H}')$, and it follows directly from the definition of the former that the diagram

$$\begin{tikzcd}
\operatorname{Ext}(A, H) \arrow[r] \arrow[d] & H^1(A, \mathfrak{H}) \arrow[d] \\
\operatorname{Ext}(A, H') \arrow[r] & H^1(A, \mathfrak{H}')
\end{tikzcd}$$

is commutative. Referring to the definition of addition in $\operatorname{Ext}(A,H)$, we conclude that the map $\operatorname{Ext}(A,H)\to H^1(A,\mathfrak{H})$ is a homomorphism.

PROPOSITION 9. *Let A,H be commutative algebraic groups with H linear and connected and let $\mathfrak{H}$ be the sheaf of germs of locally regular maps from A into H. Then the canonical map*

$$\operatorname{Ext}(A,H)\to H^1(A,\mathfrak{H})$$

is a homomorphism. If A is an abelian variety, the map is injective.

All but the last statement is known. So suppose A abelian and that $G\in\operatorname{Ext}(A,H)$ gives rise to the zero cocycle. Then there is an everywhere regular cross section $\sigma\colon A\to G$, and we may assume that $\sigma\colon 0\to 0$. The complete subvariety σA of G generates an abelian variety, so σ must be a homomorphism. Hence G is trivial.

The homomorphism of Prop. 9 is natural in the sense that the commutative diagrams in the paragraph preceding it hold. In particular, if H is a vector group, the homomorphism is a vector space homomorphism. Note that if $H=G_a$, then $\mathfrak{H}$ is the sheaf of local rings $\mathcal{O}_A$.

LEMMA. *Let A be an abelian variety, H a connected commutative linear algebraic group each of whose elements is unipotent, and $\mathfrak{H}$ the sheaf of germs of locally regular maps from A into H. Then each translation on A leaves fixed each element of $H^1(A,\mathfrak{H})$.*

The meaning of this is the following: Any $\xi\in H^1(A,\mathfrak{H})$ is determined by an open covering $\{U_i\}_{i\in I}$ of A and rational maps $\{s_{ij}\}_{i,j\in I}$ from A to H, each s_{ij} being regular on $U_i\cap U_j$, such that $s_{ij}+s_{jk}=s_{ik}$. For any $\alpha\in A$ and any rational function f on A, define the translated function $\lambda_\alpha f$ by $\lambda_\alpha f(a)=f(a-\alpha)$. The open covering $\{\alpha U_i\}$ of A and rational maps $\{\lambda_\alpha s_{ij}\}$ determine another element of $H^1(A,\mathfrak{H})$ which depends only on ξ and which we denote $\lambda_\alpha\xi$. We have to show that $\lambda_\alpha\xi=\xi$.

The lemma is trivial if $\dim H=0$. Let $\dim H=1$; then $H=G_a$ and $H^1(A,\mathfrak{H})=H^1(A,\mathcal{O}_A)$, a finite dimensional vector space over the universal domain (using, for example, [15, § 66, Th. 1] and the projective embeddibility of A [20]). For each $\alpha\in A$, λ_α is a linear transformation on $H^1(A,\mathcal{O}_A)$; let Λ_α be the matrix of λ_α corresponding to a fixed basis $\xi_1,\cdots,\xi_r$ of $H^1(A,\mathcal{O}_A)$. The map $\alpha\to\Lambda_\alpha$ is a homomorphism (not a priori rational) from A to $GL(r)$. Take an open covering $\{U_i\}$ of A, sufficiently fine so that $\xi_1,\cdots,\xi_r$ can be represented by sections $\{s_{ij}^{(1)}\},\cdots,\{s_{ij}^{(r)}\}$ regular on the respective $U_i\cap U_j$'s, and let k be a field of definition for A and each $s_{ij}^{(\nu)}$ such that each U_i is k-open. Then each $\lambda_\alpha \xi_\nu$ is represented by a covering of A by $k(\alpha)$-open subsets and sections defined over $k(\alpha)$. By the unicity of the matrix Λ_α and the algebraic nature of the cohomology, Λ_α must be invariant under all $k(\alpha)$-automorphisms of the universal domain, hence must be purely inseparable over $k(\alpha)$. Take α generic for A over k and let q be a sufficiently high power of the field characteristic ($q = 1$ if the latter is 0). Then the matrix $\Lambda_\alpha^{(q)}$ (whose terms are the q-th powers of those of Λ_α) is rational over $k(\alpha)$ and $\alpha \rightarrow \Lambda_\alpha^{(q)}$ defines a rational map from A to $GL(r)$; by [12, Th. 3] this is a homomorphism, hence trivial. Thus $\lambda_\alpha \xi = \xi$ for all α, ξ, completing the proof for $\dim H = 1$. Note that the same argument shows that each translation on A leaves fixed each element of $H^m(A, \mathcal{O}_A)$ for any $m \geqq 0$.

Now take $\dim H > 1$ and use induction. Let H_1 be a connected one-dimensional algebraic subgroup of H. The sheaf $\mathcal{H}_1$ of germs of locally regular maps of A into H_1 is a subsheaf of $\mathcal{H}$ and, since H is a fiber space over H/H_1, the quotient sheaf $\mathcal{H}/\mathcal{H}_1$ can be identified with the sheaf of germs of locally regular maps of A into H/H_1. The exact sequence

$$0 \rightarrow \mathcal{H}_1 \rightarrow \mathcal{H} \rightarrow \mathcal{H}/\mathcal{H}_1 \rightarrow 0$$

gives rise [15, § 24, Prop. 6, Cor. 1] to the exact cohomology sequence

$$H^0(A, \mathcal{H}) \rightarrow H^0(A, \mathcal{H}/\mathcal{H}_1) \rightarrow H^1(A, \mathcal{H}_1) \rightarrow H^1(A, \mathcal{H}) \rightarrow H^1(A, \mathcal{H}/\mathcal{H}_1).$$

Note that translation by an $\alpha \in A$ induces an endomorphism λ_α of each of the above cohomology groups, these endomorphisms being allowed with respect to the above exact sequence, i. e. producing the usual commutative diagram. Now $H^0(A, \mathcal{H})$ consists of all everywhere regular maps from A to H. All such maps being constant, $H^0(A, \mathcal{H})$ is isomorphic to H, and similarly $H^0(A, \mathcal{H}/\mathcal{H}_1)$ is isomorphic to H/H_1. Thus $H^0(A, \mathcal{H}) \rightarrow H^0(A, \mathcal{H}/\mathcal{H}_1)$ is surjective and we have the exact sequence

$$0 \rightarrow H^1(A, \mathcal{H}_1) \rightarrow H^1(A, \mathcal{H}) \rightarrow H^1(A, \mathcal{H}/\mathcal{H}_1).$$

Let ξ be a fixed element of $H^1(A, \mathcal{H})$. Letting τ be the last homomorphism above, for any $\alpha \in A$, our induction assumption gives $\lambda_\alpha \tau \xi = \tau \xi$, so $\tau(\lambda_\alpha \xi - \xi) = 0$, i.e., $\lambda_\alpha \xi - \xi \in H^1(A, \mathcal{H}_1)$. For any $\beta \in A$, $\lambda_\beta(\lambda_\alpha \xi - \xi) = \lambda_\alpha \xi - \xi$, so the map $\alpha \rightarrow \lambda_\alpha \xi - \xi$ is a (purely group-theoretic) homomorphism from A to $H^1(A, \mathcal{H}_1)$. Since $\mathcal{H}_1$ is isomorphic to $\mathcal{O}_A$, $H^1(A, \mathcal{H}_1)$ is a vector space with a basis $\xi_1, \cdots, \xi_r$. Choose an open covering $\{U_i\}$ of A so fine that $\xi_1, \cdots, \xi_r, \xi$ can be represented by sections $\{s_{ij}^{(1)}\}, \cdots, \{s_{ij}^{(r)}\}$, $\{s_{ij}\}$ regular on the respective $U_i \cap U_j$'s (into $H_1, \cdots, H_1, H$ respectively), and let k be a field of definition for everything here. Writing $\lambda_\alpha\xi - \xi = c_1(\alpha)\xi_1 + \cdots + c_r(\alpha)\xi_r$, for suitable (unique) constants $c_1(\alpha), \cdots, c_r(\alpha)$, we see as before that $c_1(\alpha), \cdots, c_r(\alpha)$ are invariant under all $k(\alpha)$-automorphisms of the universal domain, hence are purely inseparable over $k(\alpha)$. Again taking α to be generic for A over k and q to be a sufficiently high power of the field characteristic (or 1 if the characteristic is 0), we have $(c_i(\alpha))^q \in k(\alpha)$ for $i = 1, \cdots, r$. Again by [12, Th. 3] $\alpha \to (c_i(\alpha))^q$ is a rational homomorphism from A into G_a, hence trivial. Thus each $c_i(\alpha) = 0$, completing the proof that $\lambda_\alpha\xi = \xi$.

THEOREM 1. *Let A be an abelian variety, H a connected commutative linear algebraic group each of whose elements is unipotent, and $\mathfrak{H}$ the sheaf of germs of locally regular maps from A into H. Then the canonical homomorphism*

$$\mathrm{Ext}(A,H) \to H^1(A, \mathfrak{H})$$

is bijective.

Injectiveness has been proved in Prop. 9, so it remains only to show that any principal fiber space over A with group H can be endowed with the structure of an element of $\mathrm{Ext}(A,H)$ in a manner consistent with the fibre space structure. Let V be such a principal fiber space, $\pi\colon V \to A$ the projection. Define a *translation* on V to be a biregular map $T\colon V \to V$ such that $(Tv)h = T(vh)$ for all $v \in V$, $h \in H$ and such that $\pi Tv - \pi v$ is constant (i. e. T is a bundle map lifting to V a translation on A). The translations on V form a group, the set of maps of the form $v \to vh_0$, for fixed $h_0 \in H$, a subgroup. The lemma says merely that any translation on A can be lifted to one on V; thus the group of translations on V is transitive. Now suppose that T is a translation on V possessing a fixed point. Then $\pi Tv = \pi v$ for all $v \in V$, so if θ is the map of the locus of $v \times vh$ on $V \times V$ such that $\theta(v \times vh) = h$, we have θ defined at $Tv \times v$. But $\theta(T(vh) \times vh) = \theta(Tv \times v)$, so there exist a rational map $\phi\colon A \to H$ such that $\theta(Tv \times v) = \phi\pi v$. Since V is locally a direct product and the map $v \to \theta(Tv \times v)$ is everywhere defined, so is the map ϕ; hence ϕ is a constant, which can only be zero, so $Tv = v$. Thus there exists one and only one translation on V carrying any one given point into another. Fix a point $e \in V$ such that $\pi e = 0$. For any $v \in V$, denote by T_v the translation on V satisfying $T_v e = v$. The one-one correspondence $v \to T_v$ puts a group structure on V having e as identity element, and we have to show that this group structure is algebraic. Let k be an algebraically closed field of definition for V, H, A, the operation of H on V, and π such that e is rational over k. Let w be a generic point of V over k

and $k(x)$ the smallest overfield of k which is a field of definition for T_w[2]; then $k(x)$ is a regular extension of k containing $k(w)$ and (since T_w is unaltered by any $k(w)$-automorphism of the universal domain) purely inseparable over $k(w)$. Hence we have a variety X and generically surjective rational maps $\tau: X \rightarrow V$, $\phi: X \times V \rightarrow V$, all defined over k and the former purely inseparable, such that if $x \times v$ is generic for $X \times V$ over k then $k(x)$ is the smallest overfield of k that is a field of definition for $T_{\tau x}$ and $\phi(x \times v) = T_{\tau x}v$. We have $k(x, T_{\tau x}v) = k(x, v)$, and if y is generic for X over $k(x, v)$, then $T_{\tau x}(T_{\tau y}v) = T_{\tau z}v$ for some generic point z of X over k, z depending only on x and y (conditions TG1 and TG2′ of [21]). By Prop. 2 of [21], X is a pregroup with respect to the composition law $x \times y \rightarrow z$ and V a pretransformation space for X with composition law $x \times v \rightarrow T_{\tau x}v$. Without loss of generality, we may suppose that X is already an algebraic group. Now for any $x \in X$, the map $v \rightarrow \phi(x \times v)$ is a translation on V, since this is so whenever x is generic for X over k, and similarly, any translation on V comes in this manner from an element of X. But there exists a nonempty open subset of V which is biregularly equivalent to an open subset of a birational model of V on which X operates regularly and the translates of this open subset of V cover V. Hence X operates regularly on V: For $x \times v$ generic for $X \times V$ over k, we have $\phi(x \times v) = T_{\tau x}v$; hence $\phi(x \times e) = T_{\tau x}e = \tau x$. Thus τ is everywhere defined and the equation $\phi(x \times v) = T_{\tau x}v$ holds for all $x \in X$, $v \in V$; τ is thus a homomorphism, one-one since it is purely inseparable. The rational homomorphism $\pi\tau: X \rightarrow A$ has as kernel all $x \in X$ for which $T_{\tau x}$ is a translation by an element of H; the kernel being commutative and A abelian, X is commutative. Let x, y be independent generic points of X over k. Then $\tau(xy) = T_{\tau x}(\tau y)$ is rational over $k(x, \tau y)$. Since $xy = yx$, we get $k(\tau(xy)) \subset k(x, \tau y) \cap k(\tau x, y) = k(\tau x, \tau y)$. (For the last step, let $\{\xi_i\}$, $\{\eta_j\}$ be bases for $k(x)/k(\tau x)$ and $k(y)/k(\tau y)$ respectively, with $\xi_1 = \eta_1 = 1$, and use the fact that $\{\xi_i\eta_j\}$ is a basis for $k(x, y)/k(\tau x, \tau y)$.) Thus $T_{\tau x}$ is defined over $k(\tau x)$, so $k(\tau x) = k(x)$ and τ is birational, hence also biregular. Map H into the group V by the rule $h \rightarrow eh$. The group law on V agrees with the operation of H on V and π is now a separable rational homomorphism with kernel H, completing the proof.

---

[2] The main point of the rest of the proof is to show that $k(x)$ is actually $k(w)$. A proof different from the one that follows can be constructed by sharpening the lemma to bring in fields of rationality; we would need a result stating that a bounding cocycle that is rational over a certain field is the boundary of a cochain rational over the same field. But this would involve a lengthy re-working of parts of [15] and would take us too far afield.

The main point in the above proof, to the effect that any principal fiber space over the abelian variety A with group H is a group extension of H by A, is well known to be false if H is the multiplicative group G_m, and counterexamples can also be given if H is connected and unipotent, but not commutative.

4. Extensions of G_a by an abelian variety. If A is an abelian variety, the group $\mathrm{Ext}(A, G_a)$ has the structure of a vector space (over the universal domain), isomorphic to $H^1(A, \mathcal{O}_A)$. The following proposition will settle at the beginning all rationality questions.

PROPOSITION 10. *Let A be an abelian variety that is defined over k. Then the elements of* $\mathrm{Ext}(A, G_a)$ *arising from extensions of G_a by A that are defined over k span* $\mathrm{Ext}(A, G_a)$. *Furthermore, any number of such elements are linearly dependent only if they are linearly dependent over k.*

Let $\mathfrak{U} = \{U_i\}_{i \in I}$ be a finite open covering of A by affine subsets that are defined over k. Then $H^1(A, \mathcal{O}_A)$ and $H^1(\mathfrak{U}, \mathcal{O}_A)$ are isomorphic [15, § 47, Th. 4], so any element of $H^1(A, \mathcal{O}_A)$ can be defined by a cocycle for the covering $\mathfrak{U}$, i. e. by a set $\{f_{ij}\}_{i,j \in I}$, where f_{ij} is an everywhere regular function on $U_i \cap U_j$ and $f_{ik} = f_{ij} + f_{jk}$ for all $i, j, k \in I$. Each f_{ij} has all its poles on a k-closed subset of A, hence [17, Th. 10, p. 239] is a linear combination with constant coefficients of elements of $k(A)$. Choose constants $\alpha_1, \cdots, \alpha_N$ that are linearly independent over k and functions $f_{ij}^{(\nu)} \in k(A)$ $(i, j \in I;$ $\nu = 1, \cdots, N)$ such that $f_{ij} = \sum_{\nu=1}^{N} \alpha_\nu f_{ij}^{(\nu)}$ for all $i, j \in I$. Then $f_{ij}^{(\nu)}$ is everywhere regular on $U_i \cap U_j$ and for each $\nu = 1, \cdots, N$, $\{f_{ij}^{(\nu)}\}_{i,j \in I}$ is a cocycle for the covering $\mathfrak{U}$ of A. Thus $H^1(A, \mathcal{O}_A)$ is spanned by those of its elements that come from principal fiber spaces over A with group G_a that are defined over k. For any such fiber space V, we may choose a point $e \in V$ lying over $0 \in A$ that is rational over k and get an algebraic group structure on V having e as identity element and consistent with the fiber space structure; by the proof of Th. 1, this group structure is unique, hence invariant under all k-automorphisms of the universal domain, hence defined over a purely inseparable extension of k. (Actually, this group structure can be shown to be defined over k; cf. footnote 2). This proves the first statement of the proposition if k is algebraically closed. For any k, any extension of G_a by A that is defined over k possesses a cross section that is defined over k (G_a having k as a field of definition for its solvability), hence is describable by a factor system $f\colon A \times A \to G_a$ that is defined over k. We have proved that $\mathrm{Ext}(A, G_a)$ is spanned by elements associated with factor systems $f\colon A \times A$

$\rightarrow G_a$ that are defined over the algebraic closure of k. But for such an f, we can write $f = \sum \alpha_\nu f_\nu$, where $\{\alpha_\nu\}$ is a finite set of quantities that are linearly independent over k and where each f_ν is a function on $A \times A$ that is defined over k. Writing down the equation f satisfies as a factor system and using linear disjointness, we get that each f_ν is a factor system, which completes the proof of the first statement. It remains to show that if $f_1, \cdots, f_r$ are factor systems from $A \times A$ to G_a that are defined over k and if there exist constants $c_1, \cdots, c_r$, not all zero, such that $\sum_{i=1}^{r} c_i f_i$ is a trivial factor system, then such constants $c_1, \cdots, c_r$ may be found in k. For this, suppose $\sum_{i=1}^{r} c_i f_i(a_1, a_2) = u(a_1) + u(a_2) - u(a_1 + a_2)$, where u is a rational function on A. Each f_i being defined over k, hence having poles that are algebraic over k, we get that all the poles of u are algebraic over k. Hence there exist constants $d_1, \cdots, d_s$ and functions $u_1, \cdots, u_s$ on A that are defined over k such that $u = \sum_{i=1}^{s} d_i u_i$. Let $\alpha_1, \cdots, \alpha_N$ be a basis for the vector space over k spanned by $c_1, \cdots, c_r, d_1, \cdots, d_s$ and write $c_i = \sum_{j=1}^{N} c_{ij}\alpha_j$ for $i = 1, \cdots, r$ and $d_i = \sum_{j=1}^{N} d_{ij}\alpha_j$ for $i = 1, \cdots, s$, with each c_{ij} and d_{ij} in k. Linear disjointness gives

$$\sum_{i=1}^{r} c_{ij} f_i(a_1, a_2) = \sum_{i=1}^{s} d_{ij}(u_i(a_1) + u_i(a_2) - u_i(a_1 + a_2))$$

for each j, completing the proof.

LEMMA 1. *Let H, N be connected algebraic subgroups of the algebraic group G, with N normal in G, $G = HN$, and $H \cap N$ finite. Then the restriction to H of the natural homomorphism $G \rightarrow G/N$ is an isogeny whose degree is the Kronecker index* $\mathrm{I}(H \cdot N)$.

By [12, Prop. 2] we have an isogeny, the inseparable part q of whose degree is given by $H \cdot N = q(H \cap N)$. To get the lemma, note that the separable part of the degree of this isogeny is the number of points in $H \cap N$.

LEMMA 2. *Let the algebraic group G be an extension of $(G_a)^n$ by the abelian variety A and let the field characteristic be $p \neq 0$. Then $G = (G_a)^n B$, where B is the maximal abelian subvariety of G, and $(G_a)^n \cap B$ is finite. Furthermore, there exists an isogeny $A^{(p)} \rightarrow B$ ($A^{(p)}$ being the abelian variety got from A by taking p-th powers of coordinates) which composes with the natural isogeny $B \rightarrow A$ (restriction to B of $G \rightarrow A$) to give the map $a^{(p)} \rightarrow pa$.*

Let $\tau \colon G \rightarrow A$ be the natural homomorphism, $\sigma \colon A \rightarrow G$ a rational cross section, k a field of definition for everything, and a a generic point of A over k. The map $a \rightarrow p\sigma a$ is clearly independent of the choice of the cross section σ; since there exists such a σ that is regular over any given point of

A, we have an everywhere regular map $A \to B$, B being the image of G under the homomorphism $g \to pg$. B is clearly the maximal abelian subvariety of G, $(G_a)^n \cap B$ is finite (being both complete and linear), and $G = (G_a)^n B$ (by dimensions). But according to the theory of symmetric functions [18, Lemma 4, p. 13], the point $p\sigma a$ is rational over $k(a^{(p)})$, hence we have a homomorphism $\psi\colon A^{(p)} \to B$ and $\tau\psi a^{(p)} = \tau p\sigma a = pa$.

Note that the homomorphism $\phi\colon A^{(p)} \to A$ defined by $\phi a^{(p)} = pa$ induces a homomorphism $\phi^*\colon \mathrm{Ext}(A, G_a) \to \mathrm{Ext}(A^{(p)}, G_a)$, and Lemma 2 is practically equivalent to the statement that $\phi^* = 0$. Note also that nothing like the lemma is true in characteristic zero, for in that case, any finite subgroup of $(G_a)^n$ consists of 0 alone and the lemma can apply only to the trivial extension.

Let G be an extension of the *vector group* H by the abelian variety A. We call G *decomposable* if we can write $G = G_1 \times H'$, where G_1 is an extension of a vector subgroup H_1 of H by A and H' is a vector subgroup of H of dimension > 0; otherwise G is *indecomposable.*

LEMMA 3. *Let A be an abelian variety, H a vector group of dimension greater than A, and G an extension of H by A. Then G is decomposable.*

Let $\dim H = n$, $\dim A = \nu < n$, and first suppose that everything is defined over a perfect field k of characteristic $p \neq 0$. If a is generic for A over k, then $[k(a)\colon k(pa)] = p^{2\nu}$ and $[k(a)\colon k(a^{(p)})] = p^{\nu}$, so $[k(a^{(p)})\colon k(pa)] = p^{\nu}$. By Lemma 2, $G = HB$, B being the maximal abelian subvariety of G, and the isogeny $B \to A$ has degree dividing p^{ν}. Using the symmetry in Lemma 1, we obtain that the isogeny $H \to G/B$ also has degree dividing p^{ν}. Now use Prop. 3 to find linear coordinate functions $x_1, \cdots, x_n$ on H and additive coordinate functions $y_1, \cdots, y_n$ on G/B such that $H \to G/B$ is given by

$$y_i = x_i^{p^{\nu_i}} + (\text{a } p\text{-polynomial in } k[x] \text{ of degree} < p^{\nu_i}),\ i = 1, \cdots, n.$$

The degree of the isogeny $H \to G/B$ is $p^{\nu_1} \cdots p^{\nu_n} \leqq p^{\nu} < p^n$, so at least one of the ν_i's, say ν_1, is 0. Then $y_1 = x_1$. Let H' be the vector subgroup of H determined by $x_2 = \cdots = x_n = 0$, H_1 the vector subgroup determined by $x_1 = 0$, and $G_1 = H_1 B$. Then $G = G_1 H'$ and the homomorphism $H' \to G/G_1$ (which can be decomposed into $H' \to G/B \to (G/B)/(G_1/B)$) is given by $x_1 \to x_1$, i.e. is a biregular isomorphism, so $G = G_1 \times H'$.

It remains to consider the case of characteristic zero. For simplicity, and also to illustrate the connection of the present theory with that of differentials of the second kind, we assume, as we may, that the universal domain is the field of complex numbers and give an easy transcendental proof. Let ω be an invariant differential (of degree one) on G and $\sigma: A \rightarrow G$ a rational cross section. The induced differential $\sigma^*\omega$ on A is closed, since ω is. If $\sigma': A \rightarrow G$ is another cross section then $\sigma' a = \sigma a + fa$, where $f: A \rightarrow H$ is a rational map, and conversely, any such f defines such a σ'. We know that $\sigma'^*\omega = \sigma^*\omega + f^*\omega$ (e.g. see the last paragraph of [13]; here $(f^*\omega)(a) = \omega(fa)$), that $f^*\omega$ is exact (coming as it does from an invariant differential on H), and for any $P \in A$, such a σ' exists that is finite at P; thus $\sigma^*\omega$ differs by an exact differential from a differential that is regular at P, i.e. $\sigma^*\omega$ is of the second kind. The dimension of the space of invariant differentials on G exceeds the first Betti number of A ($\dim G = n + \nu > 2 \dim A$), so there exists an invariant $\omega \neq 0$ on G such that $\sigma^*\omega$ has zero periods. $\sigma^*\omega$ is thus exact. Also, the differential induced on H by ω is not zero (for then ω would come from an invariant differential on A, which would have to be zero), so we can modify σ to obtain $\sigma^*\omega = 0$. Taking a suitable translate of σA, we get a subvariety W of G that passes through 0, maps into A in a generically surjective fashion, and has the differential zero induced on it by ω. These same facts are then true of the algebraic group G_1 generated by W (again use last paragraph of [13]). In particular, $G_1 \neq G$, and if we set $H_1 = G_1 \cap H$, H' a vector subgroup of H complementary to H_1, we get $G = G_1 \times H'$.

PROPOSITION 11. *Let A be an abelian variety. Then there exists a vector group H of dimension $\leqq \dim A$ and an indecomposable extension Γ of H by A such that any indecomposable extension of a vector group by A is isomorphic to the quotient of Γ by a vector subgroup of H. Furthermore, if we associate to each linear functional $\psi: H \rightarrow G_a$ the extension $\psi_*\Gamma \in \operatorname{Ext}(A, G_a)$, we obtain a vector space isomorphism between the dual space of H and* $\operatorname{Ext}(A, G_a)$.

Suppose $f_i: A \times A \rightarrow G_a$, $i = 1, \cdots, n$, are factor systems. Then we get a factor system $f: A \times A \rightarrow (G_a)^n$ by setting

$$f(a_1, a_2) = (f_1(a_1, a_2), \cdots, f_n(a_1, a_2)),$$

and this can be considered as a factor system from $A \times A$ to a vector group of dimension n with a fixed linear coordinate system. Hence $f_1, \cdots, f_n$ give rise to a well-defined extension G of an n-dimensional vector group by A, and clearly any such extension G can be so obtained. We do not alter G by adding to any f_i a trivial factor system, nor are the isomorphism class of G and the vector group structure of its maximal connected linear algebraic subgroup changed by juggling $f_1, \cdots, f_n$ by a nonsingular linear transformation with constant coefficients. If $f_n = 0$, then G is the product of the extension of an $(n-1)$-dimensional vector group by A determined by $f_1, \cdots, f_{n-1}$ and the vector group G_a, i.e. G is decomposable, and conversely, if G is decomposable, then some nontrivial linear combination of $f_1, \cdots, f_n$ must be a trivial factor system; thus G is indecomposable if and only if the elements of $\mathrm{Ext}(A, G_a)$ determined by $f_1, \cdots, f_n$ (cf. Prop. 8) are linearly independent. The previous Lemma 3 now gives $\dim \mathrm{Ext}(A, G_a) \leqq \dim A$. If we construct an extension of a vector group by A by means of a set of factor systems corresponding to a basis of $\mathrm{Ext}(A, G_a)$, we get an indecomposable extension Γ of maximal dimension. It is now trivial to verify the various contentions of the proposition for this Γ.

Remark. It will be shown shortly (Th. 3) that equality holds above, i.e. $\dim H = \dim A$. Reference to the proof of the previous Lemma 3 shows that this equality, in the case of characteristic zero, implies that the dimension of the vector space of simple differentials of second kind on A modulo exact differentials is $2 \dim A$. In the case of characteristic $p \neq 0$, on the other hand, if we write $\Gamma = HB$, B being the maximal abelian subvariety of Γ we deduce that the isogeny $A^{(p)} \to B$ of Lemma 2 is actually a biregular isomorphism and that the covering $B \to A$ is exactly like $A^{(p)} \to A$, with $a^{(p)} \to pa$; furthermore, each of the ν_i in Lemma 3 must equal 1, so that there exist linear coordinate functions $x_1, \cdots, x_n$ $(n = \dim A)$ on H and additive coordinate functions $y_1, \cdots, y_n$ on Γ/B so that the isogeny $H \to \Gamma/B$ is given by

$$y_i = x_i^p + c_{i1}x_1 + \cdots + c_{in}x_n, \qquad i = 1, \cdots, n, \text{ all } c_{ij} \text{ constant.}$$

Finally, we note that in certain problems, we may not be interested in any specific vector group structure of a subgroup but merely in what we may call the *splittability* of an element $G \in \mathrm{Ext}(A, (G_a)^\nu)$, i.e. in whether or not G possesses a direct factor G_a, i.e. in whether or not G is indecomposable for *all* admissible vector group structures on $(G_a)^\nu$. Splittability can thus differ from decomposability only if $\nu > 1$ and we have characteristic $p \neq 0$. In this case, if we write $G = (G_a)^\nu B$ (with B abelian) and apply Prop. 4 (instead of 3) to the homomorphism $(G_a)^\nu \to G/B$, we get G splittable if and only if the α_1 of Prop. 4 is zero, i.e. if and only if the Lie algebra map corresponding to $(G_a)^\nu \to G/B$ is not trivial; thus G unsplittable for $\nu > 1$ means that the Lie algebra of $(G_a)^\nu$ is contained in that of B. In particular, if $\dim A > 1$ then the Γ of Prop. 11 is splittable except when all the above c_{ij} are zero, a very special case since it implies $B \cap H = 0$, and hence that A possesses only one point of order p.

Let C be a complete nonsingular curve. For the convenience of the reader, we give a brief account of the cohomology group $H^1(C, \mathcal{O}_C)$. Any element of this group is determined by an open covering $\{U_i\}_{i \in I}$ of C and a subset $\{f_{ij}\}_{i,j \in I}$ of $\Omega(C)$ (Ω being the universal domain) such that each f_{ij} is everywhere finite on $U_i \cap U_j$ and $f_{jk} - f_{ik} + f_{ij} = 0$ for all $i, j, k \in I$. Thus we can find $\{f_i\}_{i \in I}$ such that $f_{ij} = f_j - f_i$, and conversely, any set $\{U_i, f_i\}_{i \in I}$, where $\{U_i\}$ is an open covering of C, $\{f_i\} \subset \Omega(C)$, and each $f_j - f_i$ is without poles on $U_i \cap U_j$, will produce an element of $H^1(C, \mathcal{O}_C)$. To such a set $\{U_i, f_i\}$ associate a repartition $\{\tau_P\}_{P \in C}$ of $\Omega(C)$ (cf. [4]) such that $f_i - \tau_P$ is finite at P whenever $P \in U_i$. Denoting by $\Omega(C)^*$ the vector space of repartitions of C and, for any divisor $\mathfrak{A}$ of C, by $\mathcal{L}^*(\mathfrak{A})$ the subspace consisting of repartitions that are everywhere locally multiples of $-\mathfrak{A}$, we map $\{\tau_P\}$ canonically into $\Omega(C)^*/\mathcal{L}^*(0) + \Omega(C)$. One verifies directly that the resulting map $H^1(C, \mathcal{O}_C) \rightarrow \Omega(C)^*/\mathcal{L}^*(0) + \Omega(C)$ is well-defined and an Ω-linear bijection. If the genus of C is g, we deduce that $\dim H^1(C, \mathcal{O}_C) = g$. Furthermore, if $P_1, \cdots, P_g$ are distinct points of C such that the divisor $P_1 + \cdots + P_g$ is nonspecial (such points can always be found), then $\Omega(C)^* = \mathcal{L}^*(P_1 + \cdots + P_g) + \Omega(C)$, so that a basis of $H^1(C, \mathcal{O}_C)$ can be obtained from g repartitions the i-th of which ($i = 1, \cdots, g$) is everywhere finite except for a simple pole at P_i.

THEOREM 2. *Let C be a complete nonsingular curve and $\phi \colon C \rightarrow J$ the canonical map of C into its jacobian variety. Then the associated cohomology map*

$$\phi^* \colon H^1(J, \mathcal{O}_J) \rightarrow H^1(C, \mathcal{O}_C)$$

is bijective.

By Th. 1, the canonical map $\mathrm{Ext}(J, G_a) \rightarrow H^1(J, \mathcal{O}_J)$ is bijective, so we need to prove bijectivity for the composed map $\mathrm{Ext}(J, G_a) \rightarrow H^1(C, \mathcal{O}_C)$. But if g is the genus of C, then $\dim H^1(C, \mathcal{O}_C) = g$ and $\dim \mathrm{Ext}(J, G_a) \leqq g$ (Prop. 11), so only surjectivity need be proved. We shall do this by showing that for any $P \in C$, there exists a $J' \in \mathrm{Ext}(J, G_a)$ which produces an element of $H^1(C, \mathcal{O}_C)$ corresponding to a repartition of C that is everywhere finite except for a simple pole at P. Assume, as we may, that $g > 0$, let k be a field of definition for C, J, and ϕ over which P is rational, and let $\mathfrak{o}$ be the local subring of $k(C)$ consisting of all functions of the form

$$(\text{element of } k) + (\text{element of } k(C) \text{ of order} \geqq 2 \text{ at } P).$$

Let J' be the generalized jacobian variety of C corresponding to $\mathfrak{o}$, $\tau \colon J' \rightarrow J$ the natural homomorphism, and let $\phi' \colon C \rightarrow J'$ be the canonical map, all defined over k and with ϕ' normalized so that $\tau\phi'=\phi$ (cf. [9]). Fix an element $t\in k(C)$ of order 1 at P; then t is a basis for $\bar{\mathfrak{o}}/\mathfrak{o}$ ($\bar{\mathfrak{o}}$ being the integral closure of $\mathfrak{o}$ in $k(C)$) and the map $a\to\phi'((1+at))$ (a constant) is a biregular isomorphism between G_a and the kernel of τ [9, Th. 11]. Thus we can consider $J'\in \operatorname{Ext}(J,G_a)$. The element of $H^1(C,\mathcal{O}_C)$ determined by J' is given by the G_a-principal fiber space $W=\tau^{-1}(\phi C)$. The map $\phi'\colon C\to J'$ gives a cross section of W that is regular except at P. To obtain a local cross section valid in a neighborhood of P, first note that if x is a quantity that is transcendental over k, then the divisor $(t)_x$ of C is rational over $k(x)$ and any k-specialization $x\to c$ admits a unique extension to a k-specialization $(x,(t)_x)\to(c,(t)_c)$. Hence if p is generic for C over k, the positive divisor $(t)_{t(p)}-p$ specializes uniquely to $(t)_0-P$ over the k-specialization $p\to P$. Now define a rational map $\psi\colon C\to J'$, defined over k, by the rule

$$\psi p=\phi'(p-(t-t(p))) \qquad (=\phi'(p-(t)_{t(p)}+(t)_\infty)).$$

Since the divisors $(t)_\infty$ and $(t)_0-P$ are both independent of P, we deduce that the k-specialization $p\to P$ can be extended to a specialization of ψp into some point of J'. Thus ψ, which is clearly a rational cross section of W, is regular on an open neighborhood U_1 of P. The fiber space W is thus determined by the open covering of C by $U_0=C-P$ and U_1 and the single transition function $f_{01}=\psi-\phi'$. But

$$\psi p-\phi' p=\phi'(-(t-t(p)))=-\phi'((1-t/t(p)))=1/t(p)\in G_a.$$

This cohomology class is represented by the repartition of C that is $1/t$ at P and 0 elsewhere, which completes the proof.

Note that the above cohomology map ϕ^* remains unchanged if ϕ is altered by a constant translation on J; this is clear from the proof, and also follows from the Lemma to Th. 1.

LEMMA 1. *Any abelian variety is the image of a direct product of jacobian varieties under a separable rational homomorphism.*

For any variety V of dimension >0, simple point $P\in V$, and tangent vector τ to V at P, one can find a curve $C\subset V$ that has a simple point at P and is tangent to τ: it suffices to take V to be a variety in affine space and then intersect it with a suitably general linear subspace of the correct dimension passing through P and τ. Given the abelian variety A, find curves $C_1,\cdots,C_n$ on A that have simple points at 0 and whose tangent spaces there span the tangent space to A at 0. Consider the canonical map $C_i\to J_i$ of each C_i into its jacobian variety. The injection $C_i\to A$ factors into $C_i\to J_i\to A$, each map $J_i\to A$ being a rational homomorphism. Hence we have a rational homomorphism from $J_1 \times \cdots \times J_n$ into A whose corresponding Lie algebra map is surjective. This last homomorphism is thus both surjective and separable.

LEMMA 2. *If H is a finite commutative group, then the vector spaces* $\operatorname{Hom}(H, G_a)$ *and* $\operatorname{Ext}(H, G_a)$ *have a common dimension, this being zero in the case of characteristic zero and the number of generators of H/pH if the characteristic is $p \neq 0$.*

We may assume H to be cyclic of order q^n, where q is prime and $n > 0$. If q is not the field characteristic, then $\operatorname{Hom}(H, G_a) = 0$ since G_a has no element of order q^n, and $\operatorname{Ext}(H, G_a) = 0$ since G_a is divisible by q^n. So let q equal the field characteristic $p \neq 0$ and let t be a fixed generator of H. Each element of $\operatorname{Hom}(H, G_a)$ is determined by the image of t in G_a, so $\dim \operatorname{Hom}(H, G_a) = 1$. On the other hand, if $G \in \operatorname{Ext}(H, G_a)$ and $t' \in G$ is in the inverse image of t, we have $p^n t' \in G_a$, and $p^n t'$ does not depend on the choice of t'. One verifies directly that the map $\operatorname{Ext}(H, G_a) \to G_a$ defined by $G \to p^n t'$ is a vector space isomorphism, so $\dim \operatorname{Ext}(H, G_a) = 1$.

THEOREM 3. *For any abelian variety A,* $\dim \operatorname{Ext}(A, G_a) = \dim A$.

We already know that $\dim \operatorname{Ext}(A, G_a) \leqq \dim A$ (Prop. 11) with equality holding in the case of jacobian varieties (Th. 2), hence also for direct products of jacobians (Prop. 5, Cor.). Using Lemma 1, we are reduced to showing that if A is an abelian variety for which the theorem holds and B an algebraic subgroup of A, then the theorem also holds for A/B. Such being the case, Prop. 6 gives the exact sequence

$$\operatorname{Hom}(A, G_a) \to \operatorname{Hom}(B, G_a) \to \operatorname{Ext}(A/B, G_a) \to \operatorname{Ext}(A, G_a) \to \operatorname{Ext}(B, G_a).$$

But $\operatorname{Hom}(A, G_a) = 0$, so

$$\dim \operatorname{Ext}(B, G_a) - \dim \operatorname{Ext}(A, G_a) + \dim \operatorname{Ext}(A/B, G_a) - \dim \operatorname{Hom}(B, G_a) \geqq 0.$$

Now the component of the identity B_0 of B is an abelian variety, hence divisible, so we can write $B = B_0 \times H$, where H is a finite group. Since $\dim \operatorname{Ext}(B, G_a) = \dim \operatorname{Ext}(B_0, G_a) + \dim \operatorname{Ext}(H, G_a)$ and $\dim \operatorname{Hom}(B, G_a) = \dim \operatorname{Hom}(B_0, G_a) + \dim \operatorname{Hom}(H, G_a) = \dim \operatorname{Hom}(H, G_a)$, Lemma 2 implies

$$\dim \operatorname{Ext}(B_0, G_a) - \dim \operatorname{Ext}(A, G_a) + \dim \operatorname{Ext}(A/B, G_a) \geqq 0.$$

But $\dim \operatorname{Ext}(B_0, G_a) \leqq \dim B_0$, $\dim \operatorname{Ext}(A/B, G_a) \leqq \dim A/B$, and we have assumed that $\dim \operatorname{Ext}(A, G_a) = \dim A$. The fact that $\dim A = \dim A/B + \dim B_0$ implies that all inequality signs above are actually equalities.

Corollary. *If B is an algebraic subgroup of the abelian variety A, we have a natural exact sequence*

$$0 \to \mathrm{Hom}(B, G_a) \to \mathrm{Ext}(A/B, G_a) \to \mathrm{Ext}(A, G_a) \to \mathrm{Ext}(B, G_a) \to 0.$$

Appendix.

We shall use freely the conventions of [6] and [9], together with certain results in [4].

Lemma. *Let K be an algebraic function field of one variable that is separably generated over its constant field k, $\mathfrak{o}$ a semilocal subring of K, and ω a differential of K. Then ω is an $\mathfrak{o}$-differential of first kind if, whenever $z \in \mathfrak{o}$ is a separating variable for K/k, we have $\mathrm{Sp}_{K/k(z)}\omega = 0$.*

Letting ω, z be as above, for any repartition τ of $k(z)$ (hence also of K), we have $(\mathrm{Sp}_{K/k(z)}\omega)(\tau) = \omega(\tau) = \sum_P \mathrm{res}_P\, \tau\omega$, P ranging over all prime divisors of K/k. Thus $\sum_P \mathrm{res}_P\, \tau\omega = 0$ for all repartitions τ of $k(z)$. In particular, for any prime divisor p of $k(z)/k$ we have $\sum_{P \to p} \mathrm{res}_P\, z\omega = 0$. Suppose first that ω has a pole at a prime divisor Q that is prime to the places of $\mathfrak{o}$. Then there exists an element $t \in K$ such that $v_Q(t) \geqq 0$ and $\mathrm{res}_Q\, t\omega \neq 0$. Fix an element $a \in k$ that is distinct from $Q(t)$, a separating variable z_0 of K/k, and an integer n greater than the order of any pole of ω and so large that any element of K of order $\geqq n$ at each place of $\mathfrak{o}$ is in $\mathfrak{o}$. Choose $z \in K$ so that

(1) $v_Q(t - z) \geqq n$.

(2) $v_P(z - a) \geqq n$ if P is a prime divisor of $\mathfrak{o}$.

(3) $v_P(z) \geqq n$ if P is a pole of ω distinct from Q and prime to the places of $\mathfrak{o}$.

(4) $v_{P_0}(z - z_0) > 1$ for some place P_0 of K that is not a zero of dz_0.

By (4), $dz - dz_0$ has a zero at P_0, so $dz_0 \neq 0$ implies $dz \neq 0$, i.e. z is a separating variable for K/k. By (2), $z \in \mathfrak{o}$. If q is the prime divisor of $k(z)$ lying under Q and $P \neq Q$ a prime divisor of K lying over q, then (using the same letters P, Q, q to represent places) $P(z) = Q(z) = Q(t) \neq a, \infty$; by (2), we get P prime to the places of $\mathfrak{o}$ and by (3), $v_P(z\omega) \geqq 0$. Thus $\sum_{P \to q} \mathrm{res}_P\, z\omega = \mathrm{res}_Q\, z\omega = \mathrm{res}_Q\, t\omega \neq 0$, a contradiction; hence we can have poles only at the places of $\mathfrak{o}$. Thus for any $z \in \mathfrak{o}$ that is a separating variable for K/k, we have $\sum_P \mathrm{res}_P\, z\omega = 0$, P now ranging over the prime divisors of $\mathfrak{o}$. But if we add to any nonseparating variable a separating variable, we get a separating variable, so the last equation holds for all $z \in \mathfrak{o}$, precisely the condition that ω be an $\mathfrak{o}$-differential [6, Th. 8].

Remark. Even if K is not separably generated over k, a sufficient condition that ω be an $\mathfrak{o}$-differential of first kind is that $\mathrm{Sp}_{K/k(z)}\omega = 0$ for all $z \in \mathfrak{o}$ (the trace being understood to be zero if $z \in k$); this is shown by eliminating all mention of separating variables in the above proof. Conversely, if ω is an $\mathfrak{o}$-differential of first kind and $z \in \mathfrak{o}$ then we always have $\mathrm{Sp}_{K/k(z)}\omega = 0$: this is part of the Lemma to Th. 1 of [9].

In the case where the universal domain is the field of complex numbers, the following result has been proved transcendentally in [9, § 1].

PROPOSITION 12. *Let C be a complete nonsingular curve, $\mathfrak{o}$ a semilocal subring of functions on C, $\phi\colon C \to J$ the corresponding canonical map of C into its generalized jacobian variety. Then the associated map $\omega \to \phi^*\omega$ of differentials on J into differentials on C is an isomorphism between the space of invariant differentials of degree one on J and the space of $\mathfrak{o}$-differentials of first kind on C.*

We may assume that the $\mathfrak{o}$-genus π of C is > 0, for otherwise this is trivial. Let ω be an invariant differential on J and let k be an algebraically closed field of definition for C, the equivalence relation on C, J, ϕ, and ω. Let $z \in \mathfrak{o} \cap k(C)$ be a separating variable for $k(C)/k$ and write $k(C) = k(z, u)$, where $u \in k(C)$ is separably algebraic over $k(z)$. Let x be a quantity that is transcendental over k and write the divisor $(z - x)$ irredundantly as $P_1 + \cdots + P_n - Q_1 - \cdots - Q_n$. $z(P_i) = x$, $i = 1, \cdots, n$, so each P_i is generic for C over k; also each Q_i is a pole of z, hence rational over k. Since $z - x$ is a unit in $\mathfrak{o}$ we have $\phi P_1 + \cdots + \phi P_n = \phi Q_1 + \cdots + \phi Q_n$. By the last result of [13], for any point p that is rational over $k(P_1, \cdots, P_n)$, we have a differential $\omega(p)$ of $k(P_1, \cdots, P_n)/k$, and our last equation gives $\omega(\phi P_1) + \cdots + \omega(\phi P_n) = \omega(\phi Q_1) + \cdots + \omega(\phi Q_n)$. But for any $i = 1, \cdots, n$, we have $\omega(\phi P_i) = (\phi^*\omega)(P_i)$ and $\omega(\phi Q_i) = 0$, so $(\phi^*\omega)(P_1) + \cdots + (\phi^*\omega)(P_n) = 0$. For each $i = 1, \cdots, n$, $k(P_i) = k(z(P_i), u(P_i)) = k(x, u(P_i))$, so each P_i, hence also $k(P_1, \cdots, P_n)$ is separably algebraic over $k(x)$; furthermore, $P_1, \cdots, P_n$ is a complete set of conjugates over $k(x)$. Write $\phi^*\omega = y\,dz$, where $y \in k(C) = k(z, u)$. Then for $i = 1, \cdots, n$ we have $(\phi^*\omega)(P_i) = y(P_i)\,dz(P_i) = y(P_i)\,dx$, so $y(P_1)\,dx + \cdots + y(P_n)\,dx = 0$, i.e. $\mathrm{Sp}_{k(P_1)/k(x)}\, y(P_1)\,dx = 0$. In other words, $\mathrm{Sp}_{k(C)/k(z)}\phi^*\omega = 0$, proving that $\phi^*\omega$ is an $\mathfrak{o}$-differential of first kind. Now consider the sequence of rational maps $C^\pi \to C^{(\pi)} \to J$ (C^π and $C^{(\pi)}$ being the direct and symmetric products, respectively) given by $p_1 \times \cdots \times p_\pi \to p_1 + \cdots + p_\pi \to \phi p_1 + \cdots + \phi p_\pi$. For $p_1, \cdots, p_\pi$ independent generic points of C over k, we have

$$\begin{aligned}\omega(\phi p_1 + \cdots + \phi p_\pi) &= \omega(\phi p_1) + \cdots + \omega(\phi p_\pi) \\ &= (\phi^*\omega)(p_1) + \cdots + (\phi^*\omega)(p_\pi).\end{aligned}$$

Since the map $C^\pi \to J$ is generically surjective and separable, $\omega \neq 0$ implies $\phi^*\omega \neq 0$. We are through, since both vector spaces in the proposition have dimension π.

PROPOSITION 13. *Let C be a complete nonsingular curve, $\mathfrak{o}$ a semilocal subring of functions on C, J the corresponding generalized jacobian variety. Then the maximal connected linear algebraic subgroup of J is a direct product of G_a's if and only if each $\mathfrak{o}$-differential of first kind on C is a differential of second kind.*

The maximal connected linear algebraic subgroup H of J is the kernel of the natural homomorphism from J to the ordinary jacobian variety of C, hence is isomorphic to the multiplicative group of units of $\bar{\mathfrak{o}}$ modulo units of $\mathfrak{o}$, $\bar{\mathfrak{o}}$ being the integral closure of $\mathfrak{o}$. By Prop. 2, H is a product of G_a's if and only if all its elements are of order p if the characteristic is $p \neq 0$, while no element $\neq 0$ is of finite order if the characteristic is zero. If $\mathfrak{o} = \mathfrak{o}_1 \cap \mathfrak{o}_2$, where $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are semilocal subrings of functions on C with no common place, then $\bar{\mathfrak{o}} = \bar{\mathfrak{o}}_1 \cap \bar{\mathfrak{o}}_2$ and H decomposes into a direct product in the obvious way. Furthermore, the $\mathfrak{o}$-differentials of first kind are precisely the sums of $\mathfrak{o}_1$-differentials of first kind and $\mathfrak{o}_2$-differentials of first kind [6, Th. 8, Cor. 3], so it suffices to prove the proposition for $\mathfrak{o}_1$ and $\mathfrak{o}_2$ instead of $\mathfrak{o}$. Hence we may assume that $\mathfrak{o}$ is a local ring. If P, Q are distinct places of $\mathfrak{o}$, then any function on C that is very near 1 at P and very near some root of unity distinct from 1 at Q will be a unit in $\bar{\mathfrak{o}}$ some power of which is in $\mathfrak{o}$, so H will not be a product of G_a's. In this case, a differential of third kind with simple poles at P and Q and no poles elsewhere will be an $\mathfrak{o}$-differential of first kind and not of second kind. Thus we may assume that $\mathfrak{o}$ has a single place P. In characteristic zero, any $\mathfrak{o}$-differential of first kind will have zero residue at P and no poles elsewhere, hence be of second kind, while H will be a product of G_a's [9, Th. 11, Cor.]. In characteristic $p \neq 0$, the condition that H be a product of G_a's is that $f^p \in \mathfrak{o}$ for each $f \in \bar{\mathfrak{o}}$, a condition equivalent to having $\operatorname{res}_P f^p\omega = 0$ for each $f \in \bar{\mathfrak{o}}$ and each $\mathfrak{o}$-differential ω of first kind [6, Th. 8, Cor. 1]. But this is (trivially, cf. [7, Lemma 7]) equivalent to each such ω being of second kind.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] I. Barsotti, "Factor systems and differentials on abelian varieties," *Transactions of the American Mathematical Society*, vol. 84 (1957).

[2] ———, "Abelian varieties over fields of positive characteristic," *Rendiconti del Circolo Matematico di Palermo*, Series II, vol. 5 (1956).

[3] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956).

[4] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, American Mathematical Society, New York, 1951.

[5] F. Hirzebruch, *Neue Topologische Methoden in der Algebraischen Geometrie*, Berlin, 1956.

[6] M. Rosenlicht, "Equivalence relations on algebraic curves," *Annals of Mathematics*, vol. 56 (1952).

[7] ———, "Differentials of the second kind for algebraic function fields of one variable," *Annals of Mathematics*, vol. 57 (1953).

[8] ———, "Simple differentials of second kind on Hodge manifolds," *American Journal of Mathematics*, vol. 75 (1953).

[9] ———, "Generalized jacobian varieties," *Annals of Mathematics*, vol. 59 (1954).

[10] ———, "Commutative algebraic group varieties," *Algebraic Geometry and Topology, A Symposium in Honor of S. Lefschetz*, Princeton, 1957.

[11] ———, "Group varieties and differential forms," *Proceedings of the International Congress of Mathematicians* 1954, vol. III, Amsterdam, 1956.

[12] ———, "Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956).

[13] ———, "A note on derivations and differentials on algebraic varieties," *Portugaliae Mathematica*, vol. 16 (1957).

[14] ———, "Some rationality questions on algebraic groups," *Annali di Matematica Pura ed Applicata*, Series IV, vol. 43 (1957).

[15] J-P. Serre, "Faisceaux algébriques cohérents," *Annals of Mathematics*, vol. 61 (1955).

[16] ———, *Groupes Algébriques et Théorie du Corps de Classes*, mimeographed notes of course at Collège de France, 1957.

[17] A. Weil, *Foundations of Algebraic Geometry*, Colloquium Publications of the American Mathematical Society, New York, 1946.

[18] ———, *Variétés Abéliennes et Courbes Algébriques*, Paris, 1948.

[19] ———, *Fibre-Spaces in Algebraic Geometry*, mimeographed notes by A. Wallace of course at University of Chicago, 1952.

[20] ———, "On the projective embedding of abelian varieties," *Algebraic Geometry and Topology, A Symposium in Honor of S. Lefschetz*, Princeton, 1957.

[21] ———, "On algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955).

[22] ———, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (1955).

QUELQUES PROPRIÉTÉS DES VARIÉTÉS ABÉLIENNES EN CARACTÉRISTIQUE *p*.*

par JEAN-PIERRE SERRE.

à Emil Artin.

Introduction. Soit A une variété abélienne de dimension g, définie sur un corps algébriquement clos k. Lorsque $k = \boldsymbol{C}$, la variété A est un tore complexe, ce qui montre que l'algèbre de cohomologie $H^*(A, \boldsymbol{C})$ est une algèbre extérieure engendrée par $2g$ éléments de degré 1, et que l'on a $h^{r,s}(A) = \binom{g}{r} \cdot \binom{g}{s}$. On peut se demander si ces résultats cohomologiques restent valables en caractéristique $p > 0$; ils gardent un sens, à cause de leur transcription en termes de faisceaux cohérents, cf. [20]. La première question qui se posait était la détermination de $h^{0,1}(A) = \dim. H^1(A, \mathcal{O}_A)$; elle vient d'être résolue par Rosenlicht [19]. Rosenlicht montre d'abord (*loc. cit.*, Th. 1) que $H^1(A, \mathcal{O}_A)$ est isomorphe au groupe $\mathrm{Ext}(A, G_a)$ des classes d'extensions de A par le groupe additif G_a, et il prouve ensuite (*ibid.*, Th. 3) que $\mathrm{Ext}(A, G_a)$ est un k-espace vectoriel de dimension g; ce dernier résultat a été également obtenu par Barsotti [3].

De là, on passe facilement à la détermination complète de $H^*(A, \mathcal{O}_A)$, et on montre qu'une variété abélienne *n'a pas de torsion homologique* (au sens de [22]); c'est ce qui est fait au § 1. Ce § contient également un exemple de variété abélienne A dont le second groupe de cohomologie à valeurs dans les vecteurs de Witt (le groupe $H^2(A, \mathcal{W})$) *n'est pas* un module de type fini, contrairement à ce que j'avais imprudemment conjecturé dans [22]. Cet exemple n'est guère encourageant du point de vue "définition homologique des nombres de Betti"!

Le § 2 est consacré à la classification des *isogénies radicielles de hauteur* 1. On sait que les isogénies séparables $A \to A'$ correspondent aux sous-groupes finis de A; une correspondance analogue vaut pour les isogénies radicielles de hauteur 1, à condition de remplacer les sous-groupes finis de A par certaines sous-algèbres de l'algèbre de Lie de A (cf. n°. 5, Th. 3). Ce résultat n'est d'ailleurs pas nouveau: il est contenu (au moins dans le cas commutatif) dans le mémoire de Barsotti cité plus haut. Barsotti considère même des

---

* Received January 30, 1958.

isogénies de hauteur quelconque, et les classifie au moyen de la théorie de Dieudonné; ses énoncés, plus complets, sont peut-être moins maniables; c'est pourquoi j'ai cru utile de reprendre le cas de la hauteur 1, en m'appuyant uniquement sur la "théorie de Galois" de Jacobson [14]. D'ailleurs, beaucoup de questions sur les isogénies radicielles se laissent facilement ramener au cas de la hauteur 1 (cf. § 3, Lemme 9). Le § 2 se termine par une application à un théorème d'Igusa [12].

Nous rappelons au début du § 3 les principales propriétés élémentaires des groupes $\mathrm{Ext}(A,B)$ (cf. aussi [19]), et nous indiquons le comportement de ces groupes lorsque l'on effectue sur A une isogénie radicielle de hauteur 1. On en déduit une nouvelle démonstration du théorème de Barsotti [3] suivant lequel une variété abélienne *n'a pas de torsion* (dans le groupe de Néron-Severi). Le reste du § 3 est consacré à montrer que la représentation des endomorphismes de A dans $H^1(A,\mathcal{W})$, augmentée de celle dans les points d'ordre p^ν de la variété duale, est l'analogue p-adique des représentations l-adiques de Weil (voir Th. 6 et Th. 7).[1]

§ 1. Cohomologie des variétés abéliennes.

1. Structure de l'algèbre $H^*(A)$. Soit A une variété abélienne de dimension g, définie sur un corps algébriquement clos k, et soit $\mathcal{O}_A$ le faisceau de ses anneaux locaux. Posons $H^*(A)=\sum_0^\infty H^n(A,\mathcal{O}_A)$; l'opération de *cup-produit* munit l'espace vectoriel $H^*(A)$ d'une structure d'algèbre graduée; du fait que la multiplication dans $\mathcal{O}_A$ est associative et commutative, celle de $H^*(A)$ est associative et anticommutative (pour toutes les propriétés du cup-produit, nous renvoyons à l'ouvrage de Godement sur les faisceaux, [8], Chap. II, § 6).

Ce qui précède n'utilise que la structure de variété algébrique de A; utilisons maintenant sa loi de composition $s\colon A\times A\to A$. Par passage à la cohomologie, elle définit un homomorphisme $s^*\colon H^*(A)\to H^*(A\times A)$.

Mais la *formule de Künneth* s'applique au faisceau des anneaux locaux (et plus généralement à des faisceaux cohérents quelconques) : cela se voit, par exemple, en appliquant le théorème d'Eilenberg-Zilber ([8], Chap. I, Th. 3.10.1) aux complexes obtenus à partir de recouvrements affines. On a donc $H^*(A\times A)=H^*(A)\otimes H^*(A)$. De plus, le fait que A ait un élément neutre pour s montre, comme dans le cas classique, que, si $\deg(x)>0$, on a

---

[1] P. Cartier a également obtenu une telle représentation (non publié) ; sa méthode est différente: il utilise le "module de Dieudonné" de la variété duale de A à la place de $H^1(A,\mathcal{W})$.

$s^*(x) = x \otimes 1 + 1 \otimes x + \sum y_i \otimes z_i$, avec $\deg(y_i) > 0$, $\deg(z_i) > 0$. Cela signifie que $H^*(A)$ est une *algèbre de Hopf* au sens de Borel [4], § 6. Or on a:

LEMME 1. *Soit* $H = \sum_0^\infty H^n$ *une algèbre de Hopf sur* k, *associative, anticommutative, et connexe* (*i. e.* $H^0 = k$). *Soit* g *un entier tel que* $H^n = 0$ *pour* $n > g$. *On a alors* $\dim. H^1 \leqq g$, *et, si l'égalité est vérifiée, l'algèbre* H *s'identifie à l'algèbre extérieure du* k*-espace vectoriel* H^1.

D'après le théorème de structure de Borel (*loc. cit.*, Th. 6.1), l'algèbre H est produit tensoriel sur k d'algèbres monogènes $k[x_i]$. Posons $n_i = \deg(x_i)$. Le produit de tous les x_i est un élément non nul de H, de degré égal à $\sum n_i$, d'où $\sum n_i \leqq g$. En particulier, le nombre des x_i de degré 1 est $\leqq g$; comme ce nombre est visiblement égal à $\dim. H^1$, ceci démontre l'inégalité $\dim. H^1 \leqq g$. S'il y a égalité, tous les x_i sont nécessairement de degré 1; de plus leurs carrés sont nuls, car, si l'on avait $x_1^2 \neq 0$, le produit $x_1^2 \otimes x_2 \otimes \cdots \otimes x_g$ serait un élément non nul de H, de degré $g+1$, ce qui est impossible. L'algèbre H s'identifie donc bien à l'algèbre extérieure sur H^1.

Les hypothèses du lemme précédent sont vérifiées par l'algèbre de Hopf $H = H^*(A)$: on a $H^0(A) = k$ puisque A est connexe et complète, et $H^n = 0$ pour $n > g$ puisque A est de dimension g ([21], Th. 2, ou même [20], n°. 66, Th. 1 si l'on tient compte du fait qu'une variété abélienne admet un plongement projectif). On a donc l'inégalité $\dim. H^1(A, \mathcal{O}_A) \leqq g$; on notera que Rosenlicht, dans sa démonstration de *l'égalité* $\dim. H^1(A, \mathcal{O}_A) = g$ ([19], Th. 3) a d'abord besoin d'établir l'inégalité précédente (*loc. cit.*, Lemme 3). Si l'on fait maintenant usage de l'égalité en question, on obtient:

THÉORÈME 1. *Soient* A *une variété abélienne de dimension* g, *et* $\mathcal{O}_A$ *le faisceau de ses anneaux locaux. L'algèbre de cohomologie*

$$H^*(A) = \sum H^n(A, \mathcal{O}_A)$$

s'identifie à l'algèbre extérieure de l'espace vectoriel $H^1(A, \mathcal{O}_A)$, *qui est de dimension* g.

Soit Ω^r le faisceau des formes différentielles régulières de degré r sur A, et posons $h^{r,s} = \dim. H^s(A, \Omega^r)$. Du fait que le fibré tangent à une variété de groupe est trivial, le faisceau Ω^r est isomorphe à la somme directe de $\binom{g}{r}$ copies du faisceau $\mathcal{O}_A$, et l'on en déduit $h^{r,s} = \binom{g}{r} \cdot \binom{g}{s}$.

On voit en particulier que la *formule de symétrie* $h^{r,s} = h^{s,r}$ est valable pour les variétés abéliennes.

2. Absence de torsion homologique sur les variétés abéliennes. Supposons que la caractéristique p du corps de base soit > 0. On sait ([22], no. 3) que l'on peut associer à toute variété algébrique X des *opérations de Bockstein,* opérant sur $H^*(X, \mathcal{O}_X)$; on dit que X *n'a pas de torsion homologique* si ces opérations sont identiquement nulles.

Théorème 2. *Une variété abélienne n'a pas de torsion homologique.*

Soit A une variété abélienne, et soient $\beta_1, \cdots, \beta_n, \cdots$ les opérations de Bockstein associées à A. Supposons démontré que $\beta_i = 0$ pour $i < n$, et montrons que $\beta_n = 0$. Comme β_n opère sur l'algèbre de cohomologie de β_{n-1} (*loc. cit.*), on voit que, dans le cas présent, β_n opère sur $H^*(A)$. De plus β_n vérifie la formule de dérivation suivante (*loc. cit.*, formule (8)):

$$\beta_n(x \cdot y) = \beta_n(x) \cdot F^n(y) + (-1)^{\deg(x)} F^n(x) \cdot \beta_n(y), \qquad x, y \in H^*(A),$$

où F désigne l'opération définie par la puissance p-ème sur $\mathcal{O}_A$.

Puisque, en vertu du Th. 1, $H^*(A)$ est engendrée par ses éléments de degré 1, il nous suffira donc de montrer que $\beta_n(x) = 0$ si $x \in H^1(A)$. Dans ce cas, on a évidemment $s^*(x) = x \otimes 1 + 1 \otimes x$, autrement dit l'élément x est un élément *primitif* de l'algèbre de Hopf $H^*(A)$. Si l'on pose $y = \beta_n(x)$, on a $y \in H^2(A)$; de plus, en vertu du caractère fonctoriel de β_n, on a:

$$s^*(y) = s^*\beta_n(x) = \beta_n s^*(x) = \beta_n(x \otimes 1 + 1 \otimes x) = y \otimes 1 + 1 \otimes y.$$

L'élément y est donc un élément primitif de $H^*(A)$, de degré 2. Pour prouver que $y = 0$, il suffit alors d'établir le lemme suivant:

Lemme 2. *Les seuls éléments primitifs non nuls de $H^*(A)$ sont de degré* 1.

Soit $V = H^1(A)$; d'après le Théorème 1, on a $H^*(A) = \wedge V$. L'homomorphisme $s^*\colon H^*(A) \rightarrow H^*(A) \otimes H^*(A)$ s'identifie donc à l'application "diagonale" $\delta\colon \wedge V \rightarrow \wedge V \otimes \wedge V = \wedge (V + V)$.

On est alors ramené à démontrer qu'aucun élément non nul $y \in \wedge V$, de degré $\geqq 2$, ne vérifie l'identité $\delta(y) = y \otimes 1 + 1 \otimes y$. C'est là un simple exercice d'algèbre extérieure; on peut, par exemple, considérer la composante $\lambda(y)$ de $\delta(y)$ dans $\wedge V \otimes V$, et la "contracter" avec un élément v' du dual V' de V; on obtient ainsi un élément de $\wedge V$ qui n'est autre que le *produit intérieur* de y par v'; par hypothèse, on a $\lambda(y) = 0$, ce qui montre le produit intérieur de y par tout élément de V' est nul, d'où $y = 0$, comme on sait.

3. Un contre-exemple. Soit X une variété projective, et soit $\mathcal{W}_n$ le faisceaux des *vecteurs de Witt* de longueur n à coefficients dans le faisceau $\mathcal{O}_X$ des anneaux locaux de X (cf. [22], § 1). Si q est un entier $\geqq 0$, le groupe $H^q(X, \mathcal{W}_n)$ est muni de façon naturelle d'une structure de Λ-module, Λ désignant l'anneau $W(k)$ des vecteurs de Witt de longueur infinie sur le corps de base k. Lorsque n varie, les $H^q(X, \mathcal{W}_n)$ forment un système projectif, dont la limite est notée $H^q(X, \mathcal{W})$; c'est un Λ-module. Si $q = 0$, ou, si $q = 1$ et si X est normale, on sait (*loc. cit.*, Prop. 4) que $H^q(X, \mathcal{W})$ est un Λ-module *de type fini*; nous allons montrer que ce résultat *n'est plus valable pour $q = 2$, même si l'on suppose X non singulière.*

Nous prendrons pour X une variété abélienne de dimension 2, telle que l'endomorphisme $F\colon H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X)$ soit nul, par exemple le produit de deux courbes elliptiques dont l'invariant de Hasse est nul (cf. [9] ainsi que [22], § 2).

LEMME 3. *Pour tout $n \geqq 0$, l'homomorphisme*

$$F\colon H^2(X, \mathcal{W}_n) \to H^2(X, \mathcal{W}_n)$$

est nul.

Posons, pour simplifier les notations, $H_n{}^q = H^q(X, \mathcal{W}_n)$; on a en particulier $H_1{}^q = H^q(X, \mathcal{O}_X)$. Du fait que X n'a pas de torsion homologique (Théorème 2), on a une suite exacte:

$$0 \to H_{n-1}{}^q \to H_n{}^q \to H_1{}^q \to 0.$$

où le premier homomorphisme est le "décalage" V, et le second l'opération de "restriction" itérée R^{n-1}; pour la définition précise et les propriétés des opérations F, V, R, nous renvoyons à [22], § 1.

Nous raisonnerons par récurrence sur n, le cas $n = 0$ étant trivial. Puisque F et V commutent, il s'ensuit que F est nul sur $V(H_{n-1}{}^2)$; de plus, en vertu du Th. 1, $H_1{}^2$ est un espace de dimension 1, ayant pour base le cup-produit de deux éléments $x, x' \in H_1{}^1$. Choisissons alors des éléments $y, y' \in H_n{}^1$ tels que $R^{n-1}y = x$, $R^{n-1}y' = x'$; le cup-produit $y \cdot y' \in H_n{}^2$ a un sens, puisque $\mathcal{W}_n$ est un faisceau d'anneaux, et l'image de $y \cdot y'$ par R^{n-1} est $x \cdot x'$; le Λ-module $H_n{}^2$ est donc engendré par $V(H_{n-1}{}^2)$ et par $y \cdot y'$, et il nous suffira de montrer que $F(y \cdot y') = 0$.

Vu l'hypothèse faite sur X, on a $Fx = Fx' = 0$ dans $H_1{}^1$; la suite exacte écrite ci-dessus montre alors qu'il existe $z, z' \in H_{n-1}{}^1$ avec $Fy = Vz$, $Fy' = Vz'$; comme $F(y \cdot y') = Fy \cdot Fy'$, on en déduit $F(y \cdot y') = Vz \cdot Vz'$. En appliquant l'identité $Va \cdot b = V(a \cdot FRb)$, on voit que $Vz \cdot Vz' = V(z \cdot FRVz')$; mais $FRV = p$, et on obtient finalement:

$$F(y \cdot y') = Vz \cdot Vz' = V(p \cdot z \cdot z').$$

Le produit $z \cdot z'$ appartient à $H^2{}_{n-1}$; d'après l'hypothèse de récurrence il est annulé par F, et *a fortiori* par $p = RVF$; on trouve donc bien $F(y \cdot y') = 0$, ce qui achève la démonstration.

COROLLAIRE. *Le* Λ-*module* $H^2(X, \mathcal{W}) = \lim. H^2(X, \mathcal{W}_n)$ *est annulé par* p, *et ce n'est pas un module de type fini sur* Λ.

Puisque F est nul sur chaque $H^2(X, \mathcal{W}_n)$, il est nul sur leur limite projective $H^2(X, \mathcal{W})$; comme $p = FV$ sur $H^2(X, \mathcal{W})$, on voit bien que p annule $H^2(X, \mathcal{W})$; du fait que $W(k)/p \cdot W(k) = k$, cela signifie que $H^2(X, \mathcal{W})$ est un k-espace vectoriel. Le même raisonnement vaut pour chacun des $H^2(X, \mathcal{W}_n)$; de plus, la suite exacte écrite ci-dessus montre que la dimension de $H^2(X, \mathcal{W}_n)$ est n; la dimension de leur limite projective est donc infinie, cqfd.

§ 2. Isogénies radicielles de hauteur 1.

4. Résultats préliminaires. Soit G un groupe algébrique connexe, de dimension r, et soit $\mathfrak{t}(G)$ son *algèbre de Lie*, identifiée à l'espace vectoriel des champs de vecteurs tangents sur G, invariants à gauche. Soit K le corps des fonctions rationnelles sur G, et soit $\Delta(K)$ le K-espace vectoriel formé par les dérivations de K, ou, ce qui revient au même, par les champs de vecteurs tangents sur G; on démontre, comme dans la théorie classique des groupes de Lie (cf. [2], § 5 et [18], par exemple) que $\Delta(K) = \mathfrak{t}(G) \otimes_k K$; de plus, $\mathfrak{t}(G)$ est stable par l'opération de *crochet* $(X, Y) \rightarrow [X, Y]$ et l'opération de *puissance* p-*ème* $X \rightarrow X^p$, c'est une p-algèbre de Lie restreinte au sens de Jacobson (cf. [10], [13]). On notera que G opère aussi par translations à droite sur $\Delta(K)$; ces opérations laissent stable le sous-espace $\mathfrak{t}(G)$ de $\Delta(K)$, définissant ainsi la *représentation adjointe* de G.

LEMME 4. *Soit* N *un* K-*sous-espace vectoriel de* $\Delta(K)$, *et soit* $\mathfrak{n} = N \cap \mathfrak{t}(G)$; *c'est un* k-*sous-espace vectoriel de* $\mathfrak{t}(G)$.

a) *Pour que* N *soit stable par les translations à gauche de* G, *il faut et il suffit que* $N = \mathfrak{n} \otimes_k K$.

b) *Supposons* a) *vérifié. Pour que* N *soit stable par les translations à droite de* G, *il faut et il suffit que* $\mathfrak{n}$ *soit stable par la représentation adjointe de* G.

c) *Supposons* a) *vérifié. Pour que N soit stable pour le crochet et la puissance p-ème, il faut et il suffit que $\mathfrak{n}$ le soit.*

a). Si $N = \mathfrak{n} \otimes_k K$, il est clair que N est stable par les translations à gauche (nous dirons aussi "invariant à gauche"). Supposons réciproquement que cette condition soit vérifiée, et soit e_i $(1 \leqq i \leqq r)$ une base de $\mathfrak{t}(G)$ sur k, donc aussi de $\Delta(K)$ sur K. Soit E le sous-corps de K attaché à N relativement à la base e_i (cf. Bourbaki, Alg. II, § 5, déf. 2) ; d'après le Corollaire à la Prop. 10, *loc. cit.*, le corps E est contenu dans le sous-corps de K formé des fonctions invariantes par translation à gauche, sous-corps qui n'est autre que k. En appliquant alors le Th. 2, *loc. cit.*, on en déduit bien que N est engendré par $\mathfrak{n}$, d'où $N = \mathfrak{n} \otimes_k K$.

b). est évident par transport de structure.

c). On sait que $\mathfrak{t}(G)$ est stable pour le crochet et la puissance p-ème; s'il en est de même pour N, il en est donc aussi de même pour $N \cap \mathfrak{t}(G) = \mathfrak{n}$. Inversement, supposons $\mathfrak{n}$ stable pour le crochet; la formule évidente:

$$[aX, bY] = ab[X, Y] + aX(b) \cdot Y - bY(a) \cdot X, \quad a, b \in K,\ X, Y \in \Delta(K),$$

montre que N est stable pour le crochet. Supposons en outre que $\mathfrak{n}$ soit stable pour la puissance p-ème, et utilisons la formule de Hochschild (cf. par exemple [7], Lemme 4) :

$$(aX)^p = a^p X^p + (aX)^{p-1}(a) \cdot X, \qquad a \in K, \quad X \in \Delta(K).$$

En appliquant cette formule avec $X \in \mathfrak{n}$, on voit que $(aX)^p \in N$. Pour montrer que N est stable pour la puissance p-ème, il suffira donc de montrer que, si $X \in N$, $Y \in N$, $X^p \in N$, $Y^p \in N$, on a aussi $(X + Y)^p \in N$. Pour cela on utilise la formule de Jacobson (cf. [13]) :

$$(X + Y)^p = X^p + Y^p + s(X, Y), \qquad X, Y \in \Delta(K),$$

où $s(X, Y)$ est un "alternant," c'est-à-dire un polynôme (explicitement déterminé par Jacobson) par rapport à l'opération de crochet. Dans le cas qui nous occupe, on sait que l'on a $s(X, Y) \in N$, puisque N est stable pour le crochet, et il en résulte bien que $(X + Y)^p \in N$, ce qui achève la démonstration.

Remarque. Si G est *commutatif*, la représentation adjointe est triviale, et le crochet est nul dans $\mathfrak{t}(G)$. On voit donc que les sous-espaces N de $\Delta(K)$ invariants par translation et stables pour le crochet et la puissance p-ème correspondent bijectivement aux sous-espaces vectoriels $\mathfrak{n}$ de $\mathfrak{t}(G)$ stables pour la puissance p-ème.

5. Classification des isogénies radicielles de hauteur 1. Conservons les notations du n°. précédent, et soit $\phi: G \rightarrow G'$ un homomorphisme surjectif de G dans un autre groupe algébrique G'. Identifions les algèbres de Lie de G et de G', soient $\mathfrak{t}(G)$ et $\mathfrak{t}(G')$, avec les espaces tangents à l'élément neutre. L'application ϕ admet une application tangente $\mathfrak{t}(\phi): \mathfrak{t}(G) \rightarrow \mathfrak{t}(G')$, dont nous désignerons le noyau par $\mathfrak{n}(\phi)$.

D'autre part, puisque ϕ est surjectif, le corps K' des fonctions rationnelles sur G' se plonge dans le corps K; nous désignerons par $N(\phi)$ le sous-espace de $\Delta(K)$ formé des dérivations qui s'annulent sur K'.

LEMME 5. *On a* $N(\phi) = \mathfrak{n}(\phi) \otimes_k K$, *et* $\mathfrak{n}(\phi)$ *est stable pour le crochet, la puissance p-ème, et la représentation adjointe de G.*

(Nous dirons que $\mathfrak{n}(\phi)$ est une *p-sous-algèbre de Lie* de $\mathfrak{t}(G)$, stable pour la représentation adjointe).

Il est clair que $N(\phi)$ est stable pour les translations à droite et à gauche, ainsi que pour le crochet et l'opération de puissance p-ème. D'après le Lemme 4, a), on a donc $N(\phi) = \mathfrak{n} \otimes_k K$, avec $\mathfrak{n} = N(\phi) \cap \mathfrak{t}(G)$. Si $X \in \mathfrak{n}$, le vecteur tangent à l'origine X_e déterminé par le champ de vecteurs X est évidemment dans le noyau de $\mathfrak{t}(\phi)$. Réciproquement, soit X un champ de vecteurs invariant à gauche, et tel que $X_e \in \mathfrak{n}(\phi)$; par translation, on voit que X appartient en tout point de G au noyau de l'application tangente à ϕ, ce qui signifie que X appartient à $N(\phi)$; on a donc $\mathfrak{n} = \mathfrak{n}(\phi)$. En appliquant le Lemme 4, b), c), on voit alors que $\mathfrak{n}(\phi)$ est une p-sous-algèbre de Lie stable pour la représentation adjointe.

(Noter que le fait que $\mathfrak{n}(\phi)$ est stable pour la représentation adjointe implique que $\mathfrak{n}(\phi)$ est un *idéal* de $\mathfrak{t}(G)$, sans qu'il y ait équivalence entre ces propriétés).

Nous dirons que $\phi: G \rightarrow G'$ est une *isogénie radicielle* si l'extension K/K' est radicielle, c'est-à-dire si K' contient K^{p^n} pour n assez grand. Il revient au même de dire que ϕ est *bijective*, vu les propriétés connues des revêtements. L'isogénie sera dite *de hauteur 1* si l'on a $K' \supset K^p$. Le corps K^p correspond à l'isogénie "de Frobenius" $G \rightarrow G^p$, où G^p désigne la variété déduite de G par l'automorphisme $x \rightarrow x^p$ du domaine universel (au point de vue de la théorie des faisceaux, la variété G^p peut être définie comme ayant les mêmes points et la même topologie de Zariski que G, et comme faisceau d'anneaux le faisceau des puissances p-èmes de $\mathcal{O}_G$). Si $\phi: G \to G'$ est une isogénie de hauteur 1, on a donc une factorisation $G \xrightarrow{\phi} G' \to G^p$, et G' est *la normalisée de G^p dans l'extension K'/K^p* (pour les propriétés de la normalisation des variétés, voir par exemple [15], Chap. V, §§ 3, 4). La connaissance du corps K' détermine donc de manière unique l'isogénie ϕ, à un isomorphisme près, et tout revient à caractériser les corps K', avec $K \supset K' \supset K^p$, qui correspondent à des isogénies. On a tout d'abord:

LEMME 6. *Pour qu'un sous-corps K' de K, contenant K^p, corresponde à une isogénie, il faut et il suffit qu'il soit stable par les translations à gauche et à droite par les éléments de G.*

La nécessité est triviale, démontrons la suffisance. Soit G' la normalisée de G^p dans K'/K^p; tout revient à montrer que l'application $(x, y) \to xy^{-1}$ de $G \times G$ dans G définit par passage au quotient une application régulière $G' \times G' \to G'$, car on en déduira la loi de groupe de G'. Il suffit même de démontrer que $G' \times G' \to G'$ est une application rationnelle, en vertu des propriétés de la normalisation (cf. [15], Chap. V, § 3).

Nous noterons $K \circ K$ le corps des fonctions rationnelles de $G \times G$; c'est le corps des fractions de l'anneau d'intégrité $K \otimes_k K$; même chose pour $K' \circ K'$. Il nous faut démontrer que, si $f \in K'$, la fonction rationnelle $g(x, y) = f(xy^{-1})$ appartient à $K' \circ K'$. On a en tout cas $g \in K \circ K$, d'où:

$$g(x, y) = [\sum_{i=1}^{i=n} a_i(x) \otimes b_i(y)]/c(x, y), \quad \text{avec} \quad c \in K \otimes K.$$

Quitte à remplacer c par sa puissance p-ème, on peut supposer $c \in K' \otimes K'$; de plus, si l'on prend n minimum, les a_i et les b_i sont linéairement indépendants sur k. Soit U un ouvert non vide de G tel que les fonctions b_i soient régulières sur U, et que $c(x, y)$ soit une fonction rationnelle de x (non identique à ∞) pour tout $y \in U$. Les fonctions b_i sont linéairement indépendantes sur U, et il existe donc des points $y_1, \cdots, y_n \in U$ tels que la matrice $c_{ij} = b_i(y_j)$ soit inversible. Le système linéaire

$$c(x, y_j) \cdot f(xy_j^{-1}) = \sum_{i=1}^{i=n} c_{ij} a_i(x), \qquad j = 1, \cdots, n,$$

montre alors que les $a_i(x)$ sont combinaisons linéaires des fonctions $c(x, y_j) \cdot f(xy_j^{-1})$; puisque K' est invariant à droite, ces dernières fonctions appartiennent à K'. On a donc $a_i \in K'$ pour tout i, et de même $b_i \in K'$ pour tout i, cqfd.

Nous pouvons maintenant appliquer la *théorie de Jacobson* pour les extensions radicielles de hauteur 1 (cf. [14] ainsi que [11], § 1) : d'après cette théorie, les corps K' tels que $K \supset K' \supset K^p$ correspondent bijectivement aux K-sous-espaces vectoriels N de $\Delta(K)$ qui sont stables pour le crochet et la puissance p-ème. (De façon plus précise, K' et N sont annulateurs l'un de l'autre pour l'application canonique de $K \times \Delta(K)$ dans K.) Le corps K' est donc invariant à droite et à gauche si et seulement si N l'est, c'est-à-dire (Lemme 4) si N est de la forme $\mathfrak{n} \otimes_k K$, où $\mathfrak{n}$ est une p-sous-algèbre de Lie de $\mathfrak{t}(G)$ stable pour la représentation adjointe. On obtient donc finalement :

THÉORÈME 3. *Les classes d'isogénies radicielles $G \rightarrow G'$ de hauteur 1 correspondent bijectivement aux p-sous-algèbres de Lie de $\mathfrak{t}(G)$ qui sont stables pour la représentation adjointe.*

De plus, le Lemme 5 montre que la sous-algèbre $\mathfrak{n}(\phi)$ qui correspond à une isogénie ϕ n'est autre que le noyau de l'application tangente à ϕ à l'origine.

Si $\mathfrak{n}$ est une p-sous-algèbre de Lie de $\mathfrak{t}(G)$ stable pour la représentation adjointe, nous désignerons par $G/\mathfrak{n}$ le groupe G' qui lui est associé ; au point de vue ensembliste, on a $G' = G$, mais les fonctions rationnelles (resp. régulières) sur G' sont les fonctions rationnelles (resp. régulières) sur G qui sont annulées par les dérivations invariantes appartenant à $\mathfrak{n}$. D'après la théorie de Jacobson, le *degré* $\nu(\phi) = [K : K']$ de l'isogénie est égal à $p^{\dim . \mathfrak{n}}$.

Si l'on prend $\mathfrak{n} = 0$, on trouve $G/\mathfrak{n} = G$; si l'on prend $\mathfrak{n} = \mathfrak{t}(G)$, on trouve $G/\mathfrak{n} = G^p$; ce sont les deux cas extrêmes. Il peut se faire que $\mathfrak{t}(G)$ n'admette pas d'autre p-sous-algèbre de Lie, stable pour la représentation adjointe ; c'est par exemple le cas si $\mathfrak{t}(G)$ est une algèbre de Lie simple.

Si $\theta : G \rightarrow H$ est un homomorphisme, et si le noyau de l'application tangente à θ contient $\mathfrak{n}$, on peut factoriser θ en $G \rightarrow G/\mathfrak{n} \rightarrow H$: cela résulte du Lemme 5 et de la caractérisation des fonctions rationnelles sur $G/\mathfrak{n}$.

Remarques. 1) Soit $\mathfrak{n}$ une p-sous-algèbre de Lie de $\mathfrak{t}(G)$, non nécessairement stable pour la représentation adjointe ; on peut encore définir $G/\mathfrak{n}$ et montrer que la loi de composition de G définit par passage au quotient une application régulière $G \times G/\mathfrak{n} \rightarrow G/\mathfrak{n}$, d'où une structure d'*espace homogène* sur $G/\mathfrak{n}$.

2) Comme on l'a dit dans l'introduction, le Théorème 3 est essentiellement dû à Barsotti ([3], § 2), à cela près qu'il se bornait au cas des groupes commutatifs (mais il considérait des isogénies radicielles de hauteur quel-

conque). Les résultats de Barsotti ont été généralisés par Cartier; voir sa note [6], dont il faut toutefois corriger légèrement les énoncés (sauf celui du Th. 3).

6. Application à la variété d'Albanese. Soit $f\colon V \to G$ une application rationnelle d'une variété irréductible V dans un groupe algébrique commutatif G, également irréductible.

THÉORÈME 4. *Les deux propriétés suivantes sont équivalentes:*

(i) *Il est impossible de factoriser* f *en* $V \to G_1 \to G$, *où* $V \to G_1$ *est une application rationnelle, et où* $G_1 \to G$ *est une isogénie radicielle de hauteur 1 non triviale (i.e. de degré* $\neq 1$*).*

(ii) *Pour toute forme différentielle* ω *de degré 1 sur* G, *invariante par translation, et non nulle, on a* $f^*(\omega) \neq 0$.

Soit $\Omega(G)$ l'espace vectoriel des formes différentielles de degré 1 sur G qui sont invariantes par translation; c'est le dual de l'algèbre de Lie $\mathfrak{t}(G)$. On observera que, puisque G est supposé commutatif, la représentation adjointe de G dans $\mathfrak{t}(G)$ est triviale, de même que le crochet; vu la dualité entre crochet et différentielle extérieure, on a $d\omega = 0$ pour tout $\omega \in \Omega(G)$. Ainsi, *l'opération de Cartier* C est définie pour tout $\omega \in \Omega(G)$, et l'on a $C(\omega) \in \Omega(G)$, cf. [5]; cette opération est transposée de l'opération de puissance p-ème dans $\mathfrak{t}(G)$, *loc. cit.*, formule (6).

Montrons maintenant que (ii) $\Rightarrow$ (i), et soit $V \to G_1 \to G$ une factorisation de f, où $\phi\colon G \to G$ est une isogénie radicielle de hauteur 1 avec $\nu(\phi) \neq 1$. L'application $\mathfrak{t}(\phi) : \mathfrak{t}(G_1) \to \mathfrak{t}(G)$ a un noyau non nul, donc n'est pas surjective, et il existe une forme linéaire non nulle ω sur $\mathfrak{t}(G)$ qui s'annule sur l'image de $\mathfrak{t}(G_1)$; on a $\phi^*(\omega) = 0$, d'où *a fortiori* $f^*(\omega) = 0$ et cette contradiction montre bien que (ii) $\Rightarrow$ (i).

Inversement, supposons (i) vérifié, et soit $\mathfrak{n}^*$ le sous-espace de $\Omega(G)$ formé des différentielles ω telles que $f^*(\omega) = 0$. La formule $Cf^* = f^*C$ montre que $\mathfrak{n}^*$ est stable par l'opération de Cartier C, donc que l'orthogonal $\mathfrak{n}$ de $\mathfrak{n}^*$ dans $\mathfrak{t}(G)$ est stable par l'opération de puissance p-ème. Soit $G_2 = G/\mathfrak{n}$, et soit g l'application composée $V \to G \to G_2$; si $\omega' \in \Omega(G_2)$ l'image réciproque de ω' par $G \to G_2$ s'annule sur $\mathfrak{n}$, donc appartient à $\mathfrak{n}^*$, d'où $g^*(\omega') = 0$. Comme $\Omega(G_2)$ engendre en chaque point de G_2 l'espace des covecteurs tangents, on en conclut que l'application linéaire tangente à g est triviale en tout point de V où elle est définie, i.e. sur tout ouvert U de V formé de points simples et sur lequel g est régulière. Soient alors $x \in U$, $y = g(x)$, et soit $\theta \in \mathcal{O}_y(G_2)$; du fait que $g^*(d\theta) = 0$, la fonction $\theta \circ g$ est une puissance p-ème dans $\mathcal{O}_x(V)$. Munissons alors G_2 du faisceau d'anneaux formé par les puissances p^{-1}-èmes des éléments de $\mathcal{O}(G_2)$; on obtient ainsi $(G_2)^{p^{-1}}$ (cf. n°. 5), et ce qui précède montre que $g \colon V \rightarrow G_2$ est en fait une application régulière de V dans $(G_2)^{p^{-1}}$. Mais l'isogénie $G_2 \rightarrow G^p$ donne naissance à une isogénie $(G_2)^{p^{-1}} \rightarrow G$, et l'on a ainsi obtenu une factorisation de f "à travers" $(G_2)^{p^{-1}}$. Vu (i), cette isogénie doit être triviale, i. e. on doit avoir $(G_2)^{p^{-1}} = G$, ou $G_2 = G^p$, c'est-à-dire $\mathfrak{n} = \mathfrak{t}(G)$ ou encore $\mathfrak{n}^* = 0$, et (ii) est bien vérifié, cqfd.

Exemple. Soit A la *variété d'Albanese* de V; l'application canonique $f \colon V \rightarrow A$ vérifie évidemment (i), et le Théorème 4 redonne un résultat d'Igusa [12].[2]

Supposons en particulier que V soit *complète* et *normale*, et désignons par $H^0(V, \Omega^1)$ l'espace vectoriel des formes différentielles de degré 1 sur V qui n'ont pas de diviseur polaire; l'application $\omega \rightarrow f^*(\omega)$ est un homomorphisme de $\Omega(A)$ dans $H^0(V, \Omega^1)$ et est injectif d'après ce que l'on vient de voir; on obtient ainsi l'inégalité $h^{1,0} \geqq \dim. A$.

Remarques. 1) En fait, le Théorème 4 peut servir à démontrer *l'existence* de la variété d'Albanese de V. Indiquons rapidement comment:

Soit $g \colon V \rightarrow B$ une application rationnelle de V dans une variété abélienne B; on peut chercher à factoriser g en $V \rightarrow A \rightarrow B$, où $A \rightarrow B$ est une isogénie. Si l'on suppose que V engendre B, on voit aisément qu'il existe une factorisation *maximale* $V \rightarrow A \rightarrow B$; l'application $V \rightarrow A$ vérifie alors (i), et le Th. 4 montre que $\dim. A \leqq h^{1,0}$. On obtient ainsi une majoration de $\dim. B = \dim. A$ qui remplace la majoration par le genre de la courbe générique ([16], Chap. II, § 3). L'existence de la variété d'Albanese en résulte immédiatement (*loc. cit.*).

2) On observera que la condition (ii) ne signifie nullement que f soit une application *séparable*, c'est-à-dire correspondant à une extension de corps qui soit séparable: on sait que c'est inexact même pour l'application canonique de V dans sa variété d'Albanese. En voici un exemple simple: partons d'une variété abélienne A, de dimension 2, de corps des fonctions K, et soient $x, y \in K$ deux fonctions qui soient des paramètres uniformisants à l'élément neutre de A. Soit K' le sous-corps de K engendré par K^p et par l'élément $z = xy$; soit V la normalisée de A^p dans l'extension K'/K^p. On a des applica-

---

[2] Cette démonstration ne vaut qu'en caractéristique $p \neq 0$. En caractéristique zéro le théorème d'Igusa résulte simplement de ce que $\phi(V)$ *engendre* A.

tions canoniques $A \to V \to A^p$, et $[K : K'] = [K' : K^p] = p$; il s'ensuit que la variété d'Albanese de V est ou bien V ou bien A^p; mais on voit facilement que V a un point singulier à l'origine, donc V ne peut pas être une variété abélienne, et sa variété d'Albanese est A^p, ce qui fournit l'exemple cherché.

§ 3. Représentations p-adiques.

7. **Les groupes Ext(A, B).** Dans ce n°. H, nous allons résumer un certain nombre de définitions et de résultats élémentaires sur les extensions de groupes algébriques (commutatifs). Pour plus de détails, le lecteur pourra se reporter à [19], § 2 (et aussi à [2], dont le point de vue est toutefois assez différent).

Soient A, B, C trois groupes algébriques commutatifs, non nécessairement connexes. Une suite exacte d'homomorphismes (rationnels, ou réguliers, c'est la même chose) :

$$0 \to B \to C \to A \to 0 \tag{1}$$

est dite *strictement exacte* si B s'identifie à un sous-groupe de C (muni de la structure algébrique induite), et si A s'identifie au groupe quotient C/B (muni de la structure algébrique quotient). Il revient au même de dire que $B \to C$ et $C \to A$ sont *séparables*, ou encore que la suite d'algèbres de Lie:

$$0 \to \mathfrak{t}(B) \to \mathfrak{t}(C) \to \mathfrak{t}(A) \to 0 \tag{2}$$

est une suite exacte (d'espaces vectoriels).

Une suite strictement exacte (1) est appelée une *extension* de A par B; la notion d'isomorphisme de deux extensions a un sens clair; l'ensemble des classes d'extensions de A par B est noté Ext(A, B). On munit Ext(A, B) d'une loi de composition par le procédé classique de Baer [1] : si C et C' sont deux extensions, on désigne par D le sous-groupe de $C \times C'$ image réciproque de la diagonale de $A \times A$, et par Q le sous-groupe de D formé des couples $(b, -b)$, $b \in B$; on constate alors que le quotient D/Q forme de façon naturelle une extension de A par B, qui est dite somme des deux extensions données. Les raisonnements de Baer s'appliquent presque sans changement, et montrent que Ext(A, B) est un *groupe abélien* (la seule difficulté supplémentaire est qu'il faut montrer que l'on a bien des suites *strictement* exactes, mais c'est chaque fois évident sur les applications tangentes).

Si $f : A' \to A$ est un homomorphisme, et si C est une extension de A par B, on définit $f^*(C) \in \text{Ext}(A', B)$ comme le sous-groupe de $A' \times C$ formé des couples (a', c) tels que a' et c aient même image dans A. On vérifie que $f^*\colon \mathrm{Ext}(A,B) \to \mathrm{Ext}(A',B)$ est un homomorphisme, et que l'on a les formules $1^* = 1$, $(fg)^* = g^*f^*$, $(f+f')^* = f^* + f'^*$; ainsi, $\mathrm{Ext}(A,B)$ est un *foncteur contravariant additif* en A.

De même, tout homomorphisme $s\colon B \to B'$ définit un homomorphisme $s_*\colon \mathrm{Ext}(A,B) \to \mathrm{Ext}(A,B')$, et l'on montre que $\mathrm{Ext}(A,B)$ est un *foncteur covariant additif* en B. Si $f\colon A' \to A$ est un homomorphisme, on a $f^*s_* = s_*f^*$, ce qui montre que $\mathrm{Ext}(A,B)$ est *biadditif.*

Si A et B sont deux groupes algébriques commutatifs, on note $\mathrm{Hom}(A,B)$ le groupe des homomorphismes (réguliers) de A dans B.

Soit maintenant $0 \to A' \to A \to A'' \to 0$ une suite strictement exacte, et soit $\phi \in \mathrm{Hom}(A',B)$; on a $\phi_*(A) \in \mathrm{Ext}(A'',B)$, et l'on obtient ainsi un homomorphisme $d\colon \mathrm{Hom}(A',B) \to \mathrm{Ext}(A'',B)$. Cet homomorphisme de "bord," combiné avec les homomorphismes fonctoriels associés à $A' \to A$ et $A \to A''$, fournit une *suite exacte*:

$$(3) \qquad 0 \to \mathrm{Hom}(A'',B) \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(A',B) \xrightarrow{d} \mathrm{Ext}(A'',B) \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(A',B).$$

De même, on associe à toute suite strictement exacte $0 \to B' \to B \to B'' \to 0$ une *suite exacte*:

$$(4) \qquad 0 \to \mathrm{Hom}(A,B') \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,B'') \xrightarrow{d} \mathrm{Ext}(A,B') \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(A,B'').$$

8. Comportement de $\mathrm{Ext}(A,B)$ par isogénie radicielle de hauteur 1. Soient A et B deux groupes algébriques commutatifs connexes, et soit $\mathfrak{n}$ une p-sous-algèbre de Lie de $\mathfrak{t}(A)$, c'est-à-dire un sous-espace vectoriel de $\mathfrak{t}(A)$ stable pour la puissance p-ème. On a défini au n°. 5 l'isogénie radicielle $A \to A/\mathfrak{n}$; à cette isogénie nous allons associer une *suite exacte* (analogue à la suite (3) du n°. 7):

$$(5) \qquad 0 \to \mathrm{Hom}(A/\mathfrak{n},B) \to \mathrm{Hom}(A,B) \to \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B)) \xrightarrow{d} \mathrm{Ext}(A/\mathfrak{n},B) \to \mathrm{Ext}(A,B) \to \mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B)).$$

Il faut d'abord préciser que $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ et $\mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B))$ sont pris au sens de la catégorie des *espaces vectoriels munis d'une opération de puissance p-ème* (i.e. des p-algèbres de Lie abéliennes); par exemple, un élément de $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ est une application linéaire de $\mathfrak{n}$ dans $\mathfrak{t}(B)$ qui commute avec la puissance p-ème. Tout homomorphisme de A dans B définit un homomorphisme de $\mathfrak{t}(A)$ dans $\mathfrak{t}(B)$, d'où, par restriction, un homomorphisme de $\mathfrak{n}$ dans $\mathfrak{t}(B)$. Les homomorphismes $\mathrm{Hom}(A,B) \to \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ et $\mathrm{Ext}(A,B) \to \mathrm{Ext}(\mathfrak{n},\mathfrak{t}(B))$ sont définis de façon évidente. Quant à l'homomorphisme "bord" d: $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B)) \to \mathrm{Ext}(A/\mathfrak{n},B)$ il est défini ainsi: soit $\phi \in \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$, et soit $\mathfrak{n}_\phi$ le sous-espace de $\mathfrak{t}(A)\times\mathfrak{t}(B)=\mathfrak{t}(A\times B)$ formé par les couples $(X,\phi(X))$, où X parcourt $\mathfrak{n}$. Il est clair que $\mathfrak{n}_\phi$ est une p-sous-algèbre de Lie de $\mathfrak{t}(A\times B)$, ce qui permet de définir $C_\phi=(A\times B)/\mathfrak{n}_\phi$; les homomorphismes canoniques $B\to A\times B$ et $A\times B\to A/\mathfrak{n}$ définissent des homomorphismes $B\to C_\phi$ et $C_\phi\to A/\mathfrak{n}$, et l'on vérifie immédiatement que la suite

$$0\to B\to C_\phi\to A/\mathfrak{n}\to 0$$

est strictement exacte. On a ainsi obtenu l'application

$$d\colon \mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))\to\mathrm{Ext}(A/\mathfrak{n},B)$$

cherchée; on vérifie que c'est un homomorphisme.

Il reste maintenant à démontrer l'exactitude de la suite (5); jusqu'à $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$ elle est triviale. Pour $\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$, on doit montrer que les conditions "C_ϕ est isomorphe à $A/\mathfrak{n}\times B$" et "ϕ est la restriction à $\mathfrak{n}$ d'un homomorphisme de A dans B" sont équivalentes. Tout d'abord, si ϕ se prolonge en $g\colon A\to B$, l'application $a\to(a,g(a))$ de A dans $A\times B$ applique $\mathfrak{n}$ dans $\mathfrak{n}_\phi$, donc définit par passage au quotient un homomorphisme $A/\mathfrak{n}\to C_\phi$ qui est une section; on a donc bien $C_\phi=A/\mathfrak{n}\times B$. Inversement, si l'extension C_ϕ est triviale, il y a une "rétraction" $r\colon C\to B$ qui est l'identité sur B, et, en composant r avec l'application naturelle de A dans C_ϕ, on trouve un homomorphisme $g\colon A\to B$ qui prolonge $-\phi$.

Soit $\phi\in\mathrm{Hom}(\mathfrak{n},\mathfrak{t}(B))$; par construction, il existe un homomorphisme $A\to C_\phi$ relevant la projection $A\to A/\mathfrak{n}$; donc C_ϕ appartient au noyau de $\mathrm{Ext}(A/\mathfrak{n},B)\to\mathrm{Ext}(A,B)$. Inversement, si C est un élément de ce noyau, il existe un homomorphisme $k\colon A\to C$ relevant $A\to A/\mathfrak{n}$; la restriction de $-k$ à $\mathfrak{n}$ est un homomorphisme ϕ de $\mathfrak{n}$ dans $\mathfrak{t}(G)$; soit C_ϕ l'extension de $A/\mathfrak{n}$ par B associée à ϕ. L'application $(a,b)\to k(a)+b$ est un homomorphisme de $A\times B$ dans C dont la restriction à $\mathfrak{n}_\phi$ est nulle; par passage au quotient, elle définit un homomorphisme $s\colon C_\phi\to C$ qui est l'identité sur B et définit par passage au quotient l'identité sur $A/\mathfrak{n}$; les deux extensions C et C_ϕ sont donc isomorphes, ce qui démontre l'exactitude de (5) en $\mathrm{Ext}(A/\mathfrak{n},B)$.

Soit $C\in\mathrm{Ext}(A/\mathfrak{n},B)$, et soit $E\in\mathrm{Ext}(A,B)$ l'image réciproque de C par $A\to A/\mathfrak{n}$; par définition, E est le noyau de l'homomorphisme $A\times C\to A/\mathfrak{n}$ différence des homomorphismes $A\to A/\mathfrak{n}$ et $C\to A/\mathfrak{n}$. L'application

$\mathfrak{t}(A \times C) \to \mathfrak{t}(A/\mathfrak{n})$ étant surjective, la suite $0 \to E \to A \times C \to A/\mathfrak{n} \to 0$ est strictement exacte, et $\mathfrak{t}(E)$ s'identifie au noyau de $\mathfrak{t}(A) \times \mathfrak{t}(C) \to \mathfrak{t}(A/\mathfrak{n})$; il s'ensuit que $\mathfrak{t}(E)$ contient $\mathfrak{n} \times \{0\}$, et que l'élément de $\operatorname{Ext}(\mathfrak{n}, \mathfrak{t}(B))$ défini par E est trivial. Inversement, soit E une extension de A par B jouissant de cette propriété, et soit $\theta \colon \mathfrak{n} \to \mathfrak{t}(E)$ une "section" (compatible avec la puisance p-ème) ; si l'on pose $C = E/\theta(\mathfrak{n})$, on vérifie tout de suite que $C \in \operatorname{Ext}(A/\mathfrak{n}, B)$ et que l'image de C dans $\operatorname{Ext}(A, B)$ n'est autre que E, ce qui achève de démontrer l'exactitude de la suite (5).

9. Comparaison de $\operatorname{Ext}(A, B)$ avec la cohomologie de A. Nous allons maintenant reprendre, en les complétant sur quelques points, les résultats de [19], § 3. Dans tout ce qui suit, A désigne une *variété abélienne*, et B un groupe linéaire commutatif et connexe. Les deux cas que nous avons principalement en vue sont les suivants:

a) $B = G_m$, groupe *multiplicatif*,

b) $B = W_n$, groupe additif des *vecteurs de Witt* de longueur n (pour $n = 1$, c'est le groupe *additif* G_a).

Soit $\mathcal{B}$ le faisceau des germes d'applications régulières de A dans B; le groupe $H^1(A, \mathcal{B})$ n'est autre que le groupe des classes d'espaces fibrés principaux (localement triviaux) de base A et de groupe structural B. Toute extension C de A par B définit un tel espace fibré: on sait en effet ([2], Lemme 3.2 ainsi que [17], Th. 10) qu'il existe une section rationnelle $A \to C$, d'où par translation l'existence d'une section régulière en un point donné de A, ce qui montre bien que C est localement trivial. On obtient ainsi une application canonique $\theta \colon \operatorname{Ext}(A, B) \to H^1(A, \mathcal{B})$ dont on vérifie tout de suite que c'est un homomorphisme.

Lemme 7. *L'application θ est injective.*

Soit C une extension de A par B qui soit triviale en tant qu'espace fibré, c'est-à-dire qui possède une section régulière $s \colon A \to C$. Quitte à effectuer une translation, on peut supposer que $s(0) = 0$. Soit A' le sous-groupe de C engendré par $s(A)$; comme A est complète et s régulière, $s(A)$ est complète et il en est de même de A', donc aussi de $A \cap B$; comme B est une variété affine, on a donc $\dim. (A' \cap B) = 0$, d'où $\dim. A' = \dim. A = \dim. s(A)$ et $A' = s(A)$. Ainsi s est un homomorphisme, cqfd.

Remarque. Le raisonnement précédent (dû à Rosenlicht, [19], Prop. 9) démontre en fait ceci: soit V une variété complète et non singulière, et soit

$\phi: V \to A$ l'application canonique de V dans sa variété d'Albanese. L'application composée $\mathrm{Ext}(A,B) \to H^1(A,\mathcal{B}) \to H^1(V,\mathcal{B})$ est alors *injective* (le second homomorphisme étant ϕ^*). C'est là un résultat analogue à celui d'Igusa (cf. n°. 6), et qui fournit l'inégalité $\dim. A \leqq h^{0,1}$ (et même $\dim. A \leqq \dim. Z_\infty{}^1$, avec les notations de [22], n°. 7).

Soient maintenant p_1 et p_2 les deux projections de $A \times A$ sur A, et soit $s = p_1 + p_2$.

LEMME 8. *Pour qu'un élément $x \in H^1(A,\mathcal{B})$ appartienne à l'image de θ, il faut et il suffit qu'il soit "primitif," c'est-à-dire qu'il vérifie la relation:*

$$s^*(x) = p_1{}^*(x) + p_2{}^*(x) \quad \textit{dans } H^1(A \times A, \mathcal{B}).$$

La nécessité résulte de ce que $\mathrm{Ext}(A,B)$ est un foncteur *additif* de A. Supposons inversement que E soit un espace fibré principal, de base A et de groupe structural B, correspondant à un élément primitif de $H^1(A,\mathcal{B})$. Cette dernière hypothèse revient à dire qu'il existe une application régulière $g: E \times E \to E$, vérifiant la formule

$$g(e+b, e'+b') = g(e,e') + b + b',$$

et définissant par passage au quotient l'application $s: A \times A \to A$. Quitte à effectuer une translation, on peut en outre supposer que, pour un point $0 \in E$ se projetant au point 0 de A, on a $g(0,0) = 0$. Tout revient alors à montrer que la loi de composition g fait de E un groupe commutatif qui est une extension de A par B. Vérifions par exemple la commutativité de g: si $e, e' \in E$, $g(e,e')$ et $g(e',e)$ ont même image dans A, et l'on peut écrire: $g(e,e') = g(e',e) + k(e,e')$, où k est une application de $E \times E$ dans B; on voit facilement que k est régulière, et que $k(e+b, e'+b') = k(e,e')$, $b, b' \in B$; donc k définit par passage au quotient une application régulière $A \times A \to B$ qui ne peut être que constante, puisque $A \times A$ est complète et B affine; comme de plus $k(0,0) = 0$, on voit donc que $k(e,e') = 0$ pour tout couple (e,e'), ce qui démontre bien la commutativité de g. Les autres vérifications se font de manière analogue.

Les deux lemmes précédents nous permettent d'identifier $\mathrm{Ext}(A,B)$ au sous-groupe de $H^1(A,\mathcal{B})$ formé des *éléments primitifs*. Nous allons maintenant déterminer ce sous-groupe dans les deux cas particuliers indiqués plus haut:

Cas a). On a $B = G_m$, et le groupe $H^1(A,\mathcal{B})$ n'est autre que le groupe $D(A)$ des *classes de diviseurs* de la variété A, pour l'équivalence linéaire. Dire que la classe d'un diviseur X est un élément primitif de $D(A)$ signifie que l'on a $s^{-1}(X) \sim p_1^{-1}(X) + p_2^{-1}(X) = X \times A + A \times X$ sur $A \times A$, autrement dit que $X \equiv 0$ au sens de Weil [23], p. 107 (cf. aussi [16], Chap. IV). Nous désignerons par $P(A)$ le sous-groupe de $D(A)$ formé par les classses de tels diviseurs; d'après les Lemmes 7 et 8, on a $P(A) = \mathrm{Ext}(A, G_m)$, résultat dû à Weil [24].

On sait (cf. par exemple [16]) que $P(A)$ contient le sous-groupe A^* de $D(A)$ formé des classes de diviseurs *algébriquement équivalents à zéro,* le quotient $P(A)/A^*$ étant le *groupe de torsion* de A. En fait, Barsotti [3] a démontre que ce groupe est toujours nul, i.e. que $P(A) = A^*$; nous donnerons au n°. 10 une autre démonstration de ce fait.

Cas b). On a $B = W_n$, et le faisceau $\mathfrak{B}$ n'est autre *que* le faisceau $\mathfrak{B}\mathfrak{W}_n$ considéré au n°. 3. *Tout élément de $H^1(A, \mathfrak{W}_n)$ est primitif.* En effet, il suffit de montrer que $H^1(A \times A, \mathfrak{W}_n)$ est égal à $H^1(A, \mathfrak{W}_n) \times H^1(A, \mathfrak{W}_n)$; pour $n = 1$, cela résulte de la formule de Künneth (n°. 1), et on va raisonner par récurrence sur n, en utilisant la suite exacte $0 \to \mathfrak{W}_{n-1} \to \mathfrak{W}_n \to \mathcal{O} \to 0$. Les deux injections canoniques de A dans $A \times A$ définissent un homomorphisme

$$i^*: H^1(A \times A, \mathfrak{W}_n) \to H^1(A, \mathfrak{W}_n) \times H^1(A, \mathfrak{W}_n);$$

les deux projections canoniques de $A \times A$ sur A définissent un homomorphisme

$$p^*: H^1(A, \mathfrak{W}_n) \times H^1(A, \mathfrak{W}_n) \to H^1(A \times A, \mathfrak{W}_n).$$

On a $i^* \circ p^* = 1$, et tout revient à montrer que i^* est injectif. Or on a un diagramme commutatif:

$$\begin{tikzcd}
0 \arrow[r] & H^1(A \times A, \mathfrak{W}_{n-1}) \arrow[r] \arrow[d, "i^*"'] & H^1(A \times A, \mathfrak{W}_n) \arrow[r] \arrow[d, "i^*"'] & H^1(A \times A, \mathcal{O}) \arrow[d, "i^*"'] \\
0 \arrow[r] & H^1(A, \mathfrak{W}_{n-1}) \times H^1(A, \mathfrak{W}_{n-1}) \arrow[r] & H^1(A, \mathfrak{W}_n) \times H^1(A, \mathfrak{W}_n) \arrow[r] & H^1(A, \mathcal{O}) \times H^1(A, \mathcal{O}).
\end{tikzcd}$$

Vu l'hypothèse de récurrence les deux flèches verticales extrêmes sont bijectives; la flèche verticale médiane est donc injective, ce qui achève la démonstration.

On obtient finalement $\mathrm{Ext}(A, W_n) = H^1(A, \mathfrak{W}_n)$, cf. [19], Th. 1.

10. Effet d'une isogénie sur la cohomologie. Non-existence de torsion. Nous nous proposons de déterminer l'effet d'une isogénie $\phi: A \to A'$ (A et A' étant des variétés abéliennes) sur les groupes $H^1(A, \mathfrak{W}_n) = \mathrm{Ext}(A, W_n)$ et $P(A) = \mathrm{Ext}(A, G_m)$. Il est commode d'introduire quatre type "élémentaires" d'isogénies:

type s_1 (resp. s_2) : isogénie séparable $A \to A/N$, où N est un sous-groupe fini de A d'ordre premier à p (resp. d'ordre p).

type i_1 (resp. i_2) : isogénie radicielle $A \to A/\mathfrak{n}$, de hauteur 1, où $\mathfrak{n}$ est un sous-espace vectoriel de $\mathfrak{t}(A)$ ayant une base formée d'un élément X tel que $X^p = 0$ (resp. tel que $X^p = X$).

LEMME 9. *Toute isogénie est un produit d'isogénies appartenant à l'un des types précédents.*

Soit $\phi : A \to A'$ une isogénie quelconque, et soit $\nu(\phi)$ son degré; raisonnons par récurrence sur $\nu(\phi)$, le cas $\nu(\phi) = 1$ étant trivial. Si ϕ est séparable, on a $A' = A/Q$, où Q est un sous-groupe fini de A; si l'ordre de Q est premier à p, ϕ est du type s_1; sinon Q contient un sous-groupe N d'ordre p, et on peut factoriser ϕ en $A \to A/N \to A/Q$; comme le degré de l'isogénie $A/N \to A/Q$ est égal à $\nu(\phi)/p$, on peut lui appliquer l'hypothèse de récurrence. Supposons maintenant que ϕ soit inséparable, et soit $\mathfrak{q}$ le noyau de $\mathfrak{t}(A) \to \mathfrak{t}(A')$; on sait (Lemme 5) que $\mathfrak{q}$ est stable pour la puissance p-ème, et l'on a $\mathfrak{q} \neq 0$ (sinon ϕ serait séparable). La structure des p-algèbres de Lie abéliennes (c'est-à-dire la "réduction de Jordan" des applications p-linéaires) montre alors que $\mathfrak{q}$ contient un sous-espace $\mathfrak{n}$ ayant une base formée d'un élément X tel que $X^p = X$ ou $X^p = 0$ (cf. par exemple [7], nos. 10, 11). On peut alors factoriser ϕ en $A \to A/\mathfrak{n} \to A'$, et appliquer l'hypothèse de récurrence à $A/\mathfrak{n} \to A'$, cqfd.

En particulier, toute isogénie de degré p est de l'un des types s_2, i_1, ou i_2.

Si $\phi : A \to A'$ est une isogénie, nous noterons $\phi_n{}^*$ l'application de $H^1(A', \mathfrak{W}_n)$ dans $H^1(A, \mathfrak{W}_n)$ définie par ϕ; c'est un Λ-homomorphisme, Λ désignant l'anneau $W(k)$, cf. no. 3.

LEMME 10. *Si ϕ est de type s_1 ou de type i_2, $\phi_n{}^*$ est bijectif. Si ϕ est de type s_2 ou de type i_1, $\phi_n{}^*$ a pour noyau et pour conoyau des Λ-modules de longueur* 1.

D'après les Théorèmes 1 et 2, $H^1(A, \mathfrak{W}_n)$ est un Λ-module de longueur $n \dim.(A)$, et de même pour $H^1(A', \mathfrak{W}_n)$. Comme $\phi_n{}^*$ est un Λ-homomorphisme, son noyau et son conoyau ont même longueur, et il suffira de considérer le noyau.

Supposons d'abord ϕ séparable, donc de la forme $A \to A/N$. Tenant compte de ce que $H^1(A, \mathfrak{W}_n) = \mathrm{Ext}(A, W_n)$, on peut appliquer la suite exacte des Ext (cf. no. 7, suite (3)), et l'on obtient la suite exacte:[3]

$$0 \to \mathrm{Hom}(N, W_n) \to H^1(A/N, \mathfrak{W}_n) \to H^1(A, \mathfrak{W}_n). \tag{6}$$

---

[3] Cette suite exacte peut aussi se déduire de la *suite spectrale* de Cartan-Leray du revêtement galoisien $A \to A/N$.

On est alors ramené à vérifier que $\mathrm{Hom}(N, W_n)$ est un Λ-module de longueur 0 (resp. 1) dans le cas s_1 (resp. s_2), ce qui est évident.

Supposons ensuite ϕ inséparable, donc de la forme $A \to A/\mathfrak{n}$, avec $\mathfrak{n}$ de dimension 1. On peut alors appliquer la suite exacte (5) du no. 8, et l'on obtient la suite exacte:[4]

$$(7) \qquad 0 \to \mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(W_n)) \to H^1(A/\mathfrak{n}, \mathfrak{W}_n) \to H^1(A, \mathfrak{W}_n).$$

La structure de la p-algèbre de Lie $\mathfrak{t}(W_n)$ est bien connue (cf. par exemple [7], no. 16) : elle a une base formée de n éléments $X_1, \cdots, X_n$, avec $X_1{}^p = X_2$, $X_2{}^p = X_3, \cdots, X_n{}^p = 0$. On en déduit bien que $\mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(W_n))$ est de dimension 0 ou 1 (sur k) suivant que ϕ est de type i_2 ou de type i_1, cqfd.

Si $\phi\colon A \to A'$ est une isogénie, nous noterons ${}^t\phi$ l'homomorphisme de $P(A')$ dans $P(A)$ défini par ϕ (cette notation est en accord avec celle utilisée dans la théorie de la variété de Picard, cf. [16], Chap. V, § 1).

LEMME 11. *Si ϕ est de type s_2 ou de type i_1, le noyau de ${}^t\phi$ est nul; si ϕ est de type i_2, ce noyau est d'ordre p; si ϕ est de type s_1, il est fini et d'ordre premier à p. Dans tous les cas, ${}^t\phi$ est surjectif.*

On raisonne comme dans le Lemme 10, en utilisant l'isomorphisme $P(A) = \mathrm{Ext}(A, G_m)$ et les suites exactes (3) et (5). On obtient ainsi, dans le cas séparable, la suite exacte:

$$(8) \qquad 0 \to \mathrm{Hom}(N, G_m) \to P(A/N) \to P(A) \to \mathrm{Ext}(N, G_m).$$

Comme G_m est un groupe *divisible*, $\mathrm{Ext}(N, G_m)$ est nul, et ${}^t\phi$ est surjectif; quant au noyau de ${}^t\phi$, il est isomorphe à $\mathrm{Hom}(N, G_m)$, c'est-à-dire à la composante d'ordre premier à p du groupe des caractères de N; d'où le lemme dans le cas séparable.

Dans le cas inséparable, on a de même une suite exacte:

$$(9) \qquad 0 \to \mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(G_m)) \to P(A/\mathfrak{n}) \to P(A) \to \mathrm{Ext}(\mathfrak{n}, \mathfrak{t}(G_m)).$$

La p-algèbre de Lie $\mathfrak{t}(G_m)$ a comme base l'élément $Y = t\partial/\partial t$, et l'on a $Y^p = Y$; on en déduit que $\mathrm{Hom}(\mathfrak{n}, \mathfrak{t}(G_m))$ est nul (resp. cyclique d'ordre p) si l'on est dans le cas i_1 (resp. i_2), et que, dans tous les cas, $\mathrm{Ext}(\mathfrak{n}, \mathfrak{t}(G_m)) = 0$, cqfd.

THÉORÈME 5. *Une variété abélienne n'a pas de torsion.*

---

[4] De même que ci-dessus, cette suite exacte peut se déduire d'une *suite spectrale* analogue à celle de Cartan-Leray, où la cohomologie de la p-algèbre de Lie $\mathfrak{n}$ (au sens de Hochschild [10]) remplace la cohomologie des groupes.

(Autrement dit, on a $P(A) = A^*$, ou encore, si X est un diviseur, les relations "$X \equiv 0$" et "X est algébriquement équivalent à zéro" sont équivalentes).

Le groupe A^* des classes de diviseurs algébriquement équivalents à 0 est un sous-groupe de $P(A)$, et l'on sait (cf. [16], Chap. IV, par exemple) qu'il existe un entier $n \geqq 1$ tel que $n \cdot P(A) \subset A^*$. Soit $\phi \colon A \to A$ l'isogénie définie par la multiplication par n; en combinant les Lemmes 9 et 11 on voit que ${}^t\phi \colon P(A) \to P(A)$ est surjectif. Mais $P(A) = \operatorname{Ext}(A, G_m)$ et les foncteurs $\operatorname{Ext}(A, B)$ sont additifs; il s'ensuit que ${}^t\phi$ n'est autre que la multiplication par n (voir aussi [23], Prop. 31), d'où $P(A) = n \cdot P(A) \subset A^*$, cqfd.

Remarque. Comme on l'a indiqué dans l'introduction, le Théorème 5 est dû à Barsotti [3]; la démonstration de Barsotti, assez différente de celle donnée ci-dessus,[5] est basée sur une caractérisation des différentielles "logarithmiques" (voir aussi [5]).

11. Représentations p-adiques. Soit A une variété abélienne; on sait ([22], Prop. 4) que $H^1(A, \mathcal{W}) = \lim. H^1(A, \mathcal{W}_n)$ est un Λ-module libre de type fini; soit $r(A)$ son rang. Tout homomorphisme $\phi \colon A \to B$ définit un homomorphisme transposé $\phi^* \colon H^1(B, \mathcal{W}) \to H^1(A, \mathcal{W})$, limite des $\phi_n{}^*$ considérés au n°. précédent. On notera que ϕ^* *commute* aux opérations V et F.

Soit d'autre part $A^* = P(A)$ le groupe des classes de diviseurs sur A algébriquement équivalents à zéro (la "variété de Picard" de A); nous noterons $T_p(A^*)$ le "groupe de Tate" de A^* relatif au nombre premier p. Rappelons ([16], Chap. VII, § 1) que l'on a $T_p(A^*) = \operatorname{Hom}(\boldsymbol{Q}_p/\boldsymbol{Z}_p, A^*)$; un élément de $T_p(A^*)$ n'est donc pas autre chose qu'une suite $(x_1, \cdots, x_n, \cdots)$, avec $x_i \in A^*$, $px_1 = 0$, $px_2 = x_1$, $px_3 = x_2, \cdots$ etc. Si $p^{s(A)}$ est le nombre de points d'ordre p de A^* (ou de A, c'est la même chose, puisque A et A^* sont isogènes), $T_p(A^*)$ est un module libre de rang $s(A)$ sur l'anneau $\boldsymbol{Z}_p$ des entiers p-adiques (*loc. cit.*). Tout homomorphisme $\phi \colon A \to B$ définit un homomorphisme transposé ${}^t\phi \colon T_p(B^*) \to T_p(A^*)$.

On sait que l'anneau $\boldsymbol{Z}_p$ peut être identifié à l'anneau $W(\boldsymbol{F}_p)$ des vecteurs de Witt de longueur infinie sur le corps $\boldsymbol{F}_p$ à p éléments, donc à un sous-anneau de $\Lambda = W(k)$: l'ensemble des éléments de Λ invariants par F. Par extension de l'anneau d'opérateurs, le $\boldsymbol{Z}_p$-module $T_p(A^*)$ définit un Λ-module $T'_p(A^*)$ de même rang $s(A)$.

Enfin, nous désignerons par $L_p(A)$ la somme directe de $H^1(A, \mathcal{W})$ et de $T'_p(A^*)$; c'est un Λ-module libre de rang $r(A) + s(A)$, et, comme chacun de ses facteurs, c'est un foncteur contravariant additif en A. Si $\phi: A \rightarrow B$ est un homomorphisme, nous noterons ϕ' l'homomorphisme de $L_p(B)$ dans $L_p(A)$ qui lui est associé.

---

[5] Cette démonstration a également été obtenue par Cartier (non publié).

THÉORÈME 6. *Soit* $\phi: A \rightarrow B$ *une isogénie de degré* $\nu(\phi)$, *et soit* p^k *la plus haute puissance de* p *divisant* $\nu(\phi)$. *L'application* $\phi': L_p(B) \rightarrow L_p(A)$ *est alors injective, et son conoyau est un* Λ-*module de longueur finie égale à* k.

Vu le Lemme 9, il suffit de démontrer le théorème dans le cas d'une isogénie "élémentaire." Examinons successivement les quatre cas:

type s_1. Les Lemmes 10 et 11 montrent que $\phi^*: H^1(B, \mathfrak{W}) \rightarrow H^1(A, \mathfrak{W})$ ainsi que ${}^t\phi: T_p(B^*) \rightarrow T_p(A^*)$ sont bijectifs, et il en est donc de même de ϕ'; comme $k = 0$ dans ce cas, le théorème est bien vérifié.

type s_2. D'après le Lemme 10, pour tout $n \geqq 1$, le noyau et le conoyau de $\phi_n{}^*$ sont de longueur 1; par passage à la limite projective, on en déduit que le noyau de ϕ^* est de longueur 0 ou 1 (donc 0 puisque $L_p(B)$ est un module libre), et que le conoyau de ϕ^* est de longueur 1 (les conoyaux s'appliquant les uns sur les autres quand $n \rightarrow +\infty$). D'autre part, le Lemme 11 montre que ${}^t\phi$ est bijectif, d'où le théorème, puisqu'ici $k = 1$.

type i_1. Même raisonnement que pour le type s_2.

type i_2. Le Lemme 10 montre que ϕ^* est bijectif. D'autre part le Lemme 11 montre que le noyau de ${}^t\phi: B^* \rightarrow A^*$ est cyclique d'ordre p; on en déduit par le raisonnement usuel ([23], p. 50 ou [16], *loc. cit.*) que ${}^t\phi: T_p(B^*) \rightarrow T_p(A^*)$ est injectif et que son conoyau est de longueur 1, d'où le théorème, puisqu'ici encore on a $k = 1$.

COROLLAIRE 1. *Le rang* $r(A) + s(A)$ *du* Λ-*module* $L_p(A)$ *est égal à* $2.\dim(A)$.

On applique le Théorème 6 à l'isogénie $\phi: A \rightarrow A$ définie par la multiplication par p. On a $\nu(\phi) = p^{2.\dim(A)}$ ([23], p. 127), et d'autre part le conoyau de ϕ' est $L_p(A)/p \cdot L_p(A)$, qui est un Λ-module de longueur $r(A) + s(A)$.

COROLLAIRE 2. *Soient* A *et* B *deux variétés abéliennes de même dimension, et soit* ϕ *un homomorphisme de* A *dans* B. *Si* ϕ *n'est pas une isogénie, le conoyau de* ϕ' *n'est pas de longueur finie.*

Soit C l'image de A dans B. On a $\dim. C < \dim. A = \dim. B$. L'application ϕ' se factorise en $L_p(B) \rightarrow L_p(C) \rightarrow L_p(A)$. D'après le Cor. 1, le rang du Λ-module $L_p(C)$ est strictement inférieur à celui de $L_p(A)$, et le conoyau de ϕ' n'est donc pas de longueur finie.

(On pourrait facilement démontrer que $L_p(B) \rightarrow L_p(C)$ est surjectif, mais nous n'aurons pas besoin de ce résultat).

Nous allons maintenant prendre $B = A$, autrement dit considérer des éléments ϕ de l'anneau $\mathfrak{A}(A)$ des *endomorphismes* de A. A un tel élément ϕ est attaché l'endomorphisme ϕ' de $L_p(A)$; on a les formules

$$(\phi_1 + \phi_2)' = \phi_1' + \phi_2' \text{ et } (\phi_1\phi_2)' = \phi_2'\phi_1' ;$$

ces formules signifient que $\phi \rightarrow \phi'$ est une *anti-représentation* de $\mathfrak{A}(A)$ dans $L_p(A)$. Si l'on choisit une base dans $L_p(A)$, on obtient ainsi une représentation de $\mathfrak{A}(A)$ par des matrices de degré $2.\dim(A)$ à coefficients dans Λ; nous allons voir que cette représentation est l'analogue p-adique des représentations l-adiques de Weil:

THÉORÈME 7. *Si ϕ est un élément de $\mathfrak{A}(A)$, le polynôme caractéristique de ϕ (au sens de Weil,* [23], p. 131) *est égal à celui de l'endomorphisme ϕ' de $L_p(A)$ qui lui est associé. On a en particulier*

$$\nu(\phi) = \det(\phi') \quad et \quad \sigma(\phi) = \mathrm{Tr}(\phi').$$

Soit $D(\phi) = \det(\phi')$; c'est *a priori* un élément de Λ, et nous allons d'abord montrer que c'est un élément de $\boldsymbol{Z}_p$. Vu la décomposition de $L_p(A)$ en somme directe, on a $D(\phi) = \det(\phi^*) \cdot \det({}^t\phi)$, et il est clair que $\det({}^t\phi)$ appartient à $\boldsymbol{Z}_p$; reste à voir qu'il en est de même de $\det(\phi^*)$. Soit e_i, $i = 1, \cdots, r(A)$, une base de $H^1(A, \mathcal{W})$; si $\phi^*(e_i) = \sum a_{ij}e_j$, avec $a_{ij} \in \Lambda$, on a, par définition, $\det(\phi^*) = \det(a_{ij})$. Puisque $VF = p$, l'application F de $H^1(A, \mathcal{W})$ dans lui-même est une injection, et les Fe_i sont linéairement indépendants sur Λ. Du fait que ϕ^* commute avec F, on a $\phi^*(Fe_i) = \sum F(a_{ij}) \cdot Fe_i$, et l'on a $\det(\phi^*) = \det(F(a_{ij})) = F(\det(a_{ij})) = F(\det(\phi^*))$, ce qui signifie bien que $\det(\phi^*)$ est un élément de $\boldsymbol{Z}_p$, et démontre notre assertion.

A partir de là, la démonstration est la même que celle du Th. 36, p. 136, de [23]: le Th. 6 et son Cor. 2 montrent que les relations $\nu(\phi) = 0$ et $D(\phi) = 0$ sont équivalentes et que $D(\phi)$ et $\nu(\phi)$, lorsqu'ils sont non nuls, ont même valuation p-adique; en appliquant le Lemme 12, p. 134, de [23], on en déduit que $D(\phi) = \nu(\phi)$, d'où le théorème.

Remarques.

1). A la différence des représentations l-adiques ($l \neq p$), la représentation p-adique que nous venons d'obtenir est à coefficients dans $\Lambda = W(k)$, et non dans $\boldsymbol{Z}_p$; l'exemple des courbes elliptiques d'invariant de Hasse nul montre d'ailleurs qu'il est impossible d'obtenir une représentation à coefficients dans $\boldsymbol{Z}_p$ ayant la trace voulue.

2). Nous avons construit la représentation précédente comme somme directe de deux représentations. En fait on peut la décomposer de façon canonique en somme directe de *trois facteurs*: chacun des $H^1(A, W_n)$ est somme directe d'un sous-espace $H^1(A, \mathfrak{W}_n)_s$ où F est bijectif, et d'un sous-espace $H^1(A, \mathfrak{W}_n)_n$ où F est nilpotent (décomposition "de Fitting"). Par passage à la limite, on obtient une décomposition $H^1(A, \mathfrak{W})_s + H^1(A, \mathfrak{W})_n$ de $H^1(A, \mathfrak{W})$ qui est évidemment "fonctorielle"; le Λ-module $H^1(A, \mathfrak{W})_s$ est isomorphe à $\mathrm{Hom}(T_p(A), \Lambda)$, comme on peut le voir en utilisant les résultats de [22], § 3. Cette décomposition de $L_p(A)$ en trois facteurs, outre qu'elle fait jouer un rôle plus symétrique à A et A^*, a l'avantage de "séparer" les isogénies des types s_2 et i_1: celles du premier type sont bijectives sur le facteur $H^1(A, \mathfrak{W})_n$, celles du second type sur le facteur $H^1(A, \mathfrak{W})_s$.

Collège de France,
Paris.

BIBLIOGRAPHIE.

[1] R. Baer, "Erweiterungen von Gruppen und ihren Isomorphismen," *Mathematische Zeitschrift*, vol. 38 (1934), pp. 375-416.

[2] I. Barsotti, "Structure theorems for group varieties," *Annali di Matematica*, vol. 38 (1955), pp. 77-119.

[3] ———, "Abelian varieties over fields of positive characteristic," *Rendiconti del Circolo Matematico di Palermo*, vol. 5 (1956), pp. 1-25.

[4] A. Borel, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[5] P. Cartier, "Une nouvelle opération sur les formes différentielles," *Comptes Rendus*, vol. 244 (1957), pp. 426-428.

[6] ———, "Calcul différentiel sur les variétés algébriques en caractéristique non nulle," *ibid.*, vol. 245 (1957), pp. 1109-1111.

[7] J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, II," *American Journal of Mathematics*, vol. 77 (1955), pp. 218-244.

[8] R. Godement, *Topologie algébrique et théorie des faisceaux*, Paris, Hermann, 1958.

[9] H. Hasse, " Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p," *Journal Crelle*, vol. 172 (1934), pp. 77-85.

[10] G. Hochschild, " Cohomology of restricted Lie algebras," *American Journal of Mathematics*, vol. 76 (1954), pp. 555-580.

[11] ———, " Simple algebras with purely inseparable splitting fields of exponent 1," *Transactions of the American Mathematical Society*, vol. 79 (1955), pp. 477-489.

[12] J. Igusa, "A fundamental inequality in the theory of Picard varieties," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 41 (1955), pp. 317-320.

[13] N. Jacobson, "Abstract derivation and Lie algebras," *Transactions of the American Mathematical Society*, vol. 42 (1937), pp. 206-224.

[14] ———, " Galois theory of purely inseparable fields of exponent 1," *American Journal of Mathematics*, vol. 66 (1944), pp. 645-648.

[15] S. Lang, *Introduction to algebraic geometry*, Interscience Tracts n° 5, New York, 1958.

[16] ———, *Abelian varieties*, Interscience Tracts, New York, 1958.

[17] M. Rosenlicht, " Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp .401-443.

[18] ———, "A note on derivations and differentials on algebraic varieties," *Portugaliae Mathematica*, vol. 16 (1957), pp. 43-55.

[19] ———, " Extensions of vector groups by abelian varieties," *American Journal of Mathematics*, vol. 80 (1958), pp. 685-713.

[20] J-P. Serre, " Faisceaux algébriques cohérents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.

[21] ———, " Sur la cohomologie des variétés algébriques," *Journal de Mathématiques*, vol. 36 (1957), pp. 1-16.

[22] ———, " Sur la topologie des variétés algébriques en caractéristique p," *Symposium de topologie algébrique*, Mexico, 1956.

[23] A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, Hermann, 1948.

[24] ———, " Variétés abéliennes," *Colloque d'algèbre et théorie des nombres*, Paris, 1949, pp. 125-128.

LIE GROUPS AND LIE HYPERALGEBRAS OVER A FIELD OF CHARACTERISTIC $p > 0$ (VIII).[*] [†]

By JEAN DIEUDONNÉ.

To E. Artin on his sixtieth birthday.

1. Introduction. In the last two papers of this series,[1] we obtained some precise information on what one may call the "building blocks" in the theory of formal Lie groups (over an algebraically closed field), namely the *simple* ones: thanks to the fundamental work of Chevalley [3], the simple noncommutative Lie groups are now known up to isomorphism, and the simple abelian groups have been determined in [10] up to isogeny. The main task ahead is now to see how these blocks are assembled in the most general groups, in other words, to study the problem of *extensions* of formal Lie groups. This paper is a small beginning in that direction: we have concentrated our efforts on the question of the position of the simple "divisible" abelian subgroups (i.e. the simple groups other than the additive group I_∞) in an arbitrary group; it is known that (with the exception of the tori) they lie in the center of the group, and the natural conjecture is that those which are in the center are quasi-direct factors of the whole group. I am able in this paper to prove that conjecture for *solvable* groups; the general theorem (if true) is linked with what seems to me the biggest open question remaining in the theory, the generalization of Levi's theorem.

Group extensions nowadays means cohomology, and we have followed the obvious method of attack, which consists in developing and using in our case

---

[*] Received March 4, 1958.

[†] Work done under contract AF 49(638)-106 with the U. S. Air Force.

[1] I use the terminology and results of these papers ([4] to [10]), and take this opportunity of correcting a few inaccuracies in [9] and [10]. In [9], p. 348, line 6, there should be a bar on the first u. On p. 352, the proof of (v) is not explicit enough: it should be observed that $[\mathfrak{g}_{r+1} \cap \mathfrak{H}, \mathfrak{t}_r]$ is contained in $\mathfrak{t}_r$, for we have $[\mathfrak{g}_{r+1} \cap \mathfrak{H}, \mathfrak{z}_r \cap \mathfrak{H}] \subset \mathfrak{z}_r \cap \mathfrak{H}$, and $[\mathfrak{u}_{r+1}, \mathfrak{z}_r \cap \mathfrak{N}] \subset \mathfrak{t}_r$ by (ii); hence $[X + T + U, U'] \in \mathfrak{t}_r$, and similarly $[U, X' + T'] \in \mathfrak{t}_r$. On p. 371, line 13, read $\bar{x}^\beta$ instead of x^β. On p. 376, section 19, the field K has to be algebraically closed throughout. On p. 381, line 10 from bottom, read H^* instead of H. On p. 382, line 10, read "equal to C." In [10], p. 114, line 2, read [4] instead of [3]; in footnote 3, line 3, read $G_{n,m,r}$ instead of $G_{m,n,}$. On p. 130, line 5, read $ms - j$ instead of $ms + j$.

the well-established cohomological notions which have proved their value in so many other theories. In our peculiar set-up, everything, of course, has first to be "formalized," in order to be able to do without set-theoretical concepts; but if this is done in the most trivial way for cross-sections (whose existence constitutes such a thorny problem in the case of algebraic groups), various technical difficulties arise in the extension of other basic concepts; I only mention here the absence of any sensible definition of 0-cochains (which is particularly troublesome for the low dimensional cohomology groups, in which we are especially interested), and the apparent necessity of introducing infinite-dimensional Lie groups as auxiliary tools, with all the extra care which is required when handling these somewhat elusive objects. Unfortunately, the so-called foundational books and papers on cohomology are, as usual, inadequate to cope with this new situation: they constitute at best a blueprint which one has to follow through endless tedious verifications, but do not provide any ready-made axiomatics which would dispense altogether with this unpleasant work; it is to be hoped that the more abstract homological algebra now in gestation in several quarters will fare better in this respect.

As a by-product of our investigation, it is, in particular, possible to give a complete description of all *two-dimensional* Lie groups over an algebraically closed field; apart from a satisfaction of mere curiosity, they provide unexpected counter-examples for several pleasant and plausible conjectures: for instance, an extension of the additive group by itself may very well be a non representable Lie group. This "pathology" seems to put strong limitations to the use of the theory of algebraic groups (as exemplified in [9]) to derive properties of formal Lie groups, and the unduly optimistic outlook expressed at the end of the introduction of [9] is no longer tenable.

2. Infinite dimensional formal Lie groups. It will be necessary for our purpose, to extend first the notion of formal Lie group to groups of "infinite dimension" in a manner which differs from the previous extensions of that type made in [6] and (by implication) in [8, no. 2]. Let I be an arbitrary set, and $\boldsymbol{x} = (x_i)_{i \in I}$ a set of indeterminates. When in the following we speak of a *power series* in the x_i with coefficients in a field K, we will *not* mean the most general power series in these indeterminates (as defined in [6, no. 2]), but only those series in which, for every integer $m \geqq 0$, there are only a *finite number of terms of total degree* $\leqq m$; these series obviously form a subalgebra of the algebra of all power series in the x_i, and it is *that* subalgebra which, by abuse of notation, we will write $K[[\boldsymbol{x}]]$ or $K[[x_i]]_{i \in I}$.

A fundamental consequence of that definition is that, if $(u_i)_{i\in I}$ is a family of elements of $K[[\boldsymbol{y}]]$ (where $\boldsymbol{y}=(y_j)_{j\in J}$), which are power series without constant terms, then it is possible to *substitute* the u_i to the x_i in any power series $v\in K[[\boldsymbol{x}]]$, and the resulting power series still belongs to $K[[\boldsymbol{y}]]$.

We can then define a formal Lie group of *dimension* Card(I) exactly as a formal Lie group of finite dimension, as well as the notion of homomorphism of a formal Lie group into another one (both of arbitrary dimension), by replacing power series in two sets of n indeterminates by power series (in the sense defined above) in two sets of indeterminates indexed by I, in the definitions given in [4, no. 2 and no. 3]. The existence of the "inverse" $\boldsymbol{x}^{-1}=(\theta_i(\boldsymbol{x}))$ in such a group G follows as in the finite dimensional case, the terms of total degree m in the power series θ_i being determined by induction on m. A similar argument proves the following

LEMMA 1. *Let (J,L) be an arbitrary partition of I. There exist two uniquely determined systems of power series without constant terms $\boldsymbol{u}(\boldsymbol{x})=(u_i(\boldsymbol{x}))_{i\in I}$ and $\boldsymbol{v}(\boldsymbol{x})=(v_i(\boldsymbol{x}))_{i\in I}$ such that $u_k(\boldsymbol{x})=0$ for $k\in L$, $v_j(\boldsymbol{x})=0$ for $j\in J$, and*

$$\boldsymbol{u}(\boldsymbol{x})\boldsymbol{v}(\boldsymbol{x})=\boldsymbol{x}. \tag{1}$$

Indeed, these conditions amount to the system of equations

$$u_j+\psi_j(\boldsymbol{u},\boldsymbol{v})=x_j \quad \text{for } j\in J,$$

$$v_k+\psi_k(\boldsymbol{u},\boldsymbol{v})=x_k \quad \text{for } k\in L,$$

where the ψ_i are power series all of whose terms have a total degree $\geqq 2$, and these have obviously a unique solution.

We observe that there is in general no hyperalgebra (in the usual sense, see for instance [8, no. 2]) corresponding to a formal Lie group of arbitrary dimension; this is due to the fact that if we write as usual $(\phi(\boldsymbol{x},\boldsymbol{y}))^{\gamma}=\sum_{\alpha,\beta} d_{\alpha\beta\gamma}\boldsymbol{x}^{\alpha}\boldsymbol{y}^{\beta}$, when α and β are given, there may well be an infinity of indices γ for which $d_{\alpha\beta\gamma}\neq 0$, hence the product of two left-invariant semi-derivations Z_α, Z_β on G will not in general be a finite linear combination of the Z_γ.

However, the main results which we shall need can be proved directly without the use of the hyperalgebras. If J is a subset of I, we say that J corresponds to a *typical subgroup* of G if the following condition is satisfied: for any system $(y_j)_{j\in J}=\boldsymbol{y}$ of indeterminates, define $\boldsymbol{j}(\boldsymbol{y})=(j_i(\boldsymbol{y}))$ as the system of power series $j_i(\boldsymbol{y})=y_i$ for $i\in J$, $j_i(\boldsymbol{y})=0$ otherwise; then we must have $\phi_i(\boldsymbol{j}(\boldsymbol{y}),\boldsymbol{j}(\boldsymbol{z}))=0$ for all indices $i \notin J$. If we write $\phi'_i(\boldsymbol{y},\boldsymbol{z}) = \phi_i(\boldsymbol{j}(\boldsymbol{y}),\boldsymbol{j}(\boldsymbol{z}))$ for $i \in J$, the system of power series ϕ'_i defines a group law, and if we denote by H that formal Lie group, $\boldsymbol{j}$ is a homomorphism, which is called the natural injection of H into G. We say that H is a *normal* subgroup if the components of $\boldsymbol{x}\boldsymbol{j}(\boldsymbol{y})\boldsymbol{x}^{-1}$ of index $k \notin J$ are all 0; we can then write $\boldsymbol{x}\boldsymbol{j}(\boldsymbol{y})\boldsymbol{x}^{-1} = \boldsymbol{j}(\boldsymbol{u}(\boldsymbol{x},\boldsymbol{y}))$, where $\boldsymbol{u}(\boldsymbol{x},\boldsymbol{y}) = u_j(\boldsymbol{x},\boldsymbol{y}))_{j\in J}$ is a system of power series without constant terms. When H is a normal typical subgroup of G, we now proceed to define the *quotient group* G/H. Using Lemma 1, there exist two well determined systems of power series $\boldsymbol{r}(\boldsymbol{x}) = (r_j(\boldsymbol{x}))_{j\in J}$ and $\boldsymbol{h}(\boldsymbol{x}) = (h_i(\boldsymbol{x}))_{i\in I}$ such that $h_i(\boldsymbol{x}) = 0$ for $i \in J$ and $\boldsymbol{x} = \boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))\boldsymbol{h}(\boldsymbol{x})$. If $\boldsymbol{y} = (y_i)$ is a second "generic point" of G, we can therefore write

$$\boldsymbol{x}\boldsymbol{y}^{-1} = \boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))\boldsymbol{h}(\boldsymbol{x})\boldsymbol{j}(\boldsymbol{r}(\boldsymbol{y}^{-1}))\boldsymbol{h}(\boldsymbol{y}^{-1}),$$

and using the fact that H is normal, this can also be written

$$\begin{aligned}\boldsymbol{x}\boldsymbol{y}^{-1} &= \boldsymbol{j}(\boldsymbol{u}^{(1)}(\boldsymbol{x},\boldsymbol{y}))\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y}^{-1})\\ &= \boldsymbol{j}(\boldsymbol{u}^{(2)}(\boldsymbol{x},\boldsymbol{y}))\boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y}^{-1})),\end{aligned}$$

where $\boldsymbol{u}^{(1)}$ and $\boldsymbol{u}^{(2)}$ are systems of power series; hence, replacing $\boldsymbol{x}$ by $\boldsymbol{x}\boldsymbol{y}$ in that identity, we get

$$\boldsymbol{x} = \boldsymbol{j}(\boldsymbol{u}^{(2)}(\boldsymbol{x}\boldsymbol{y},\boldsymbol{y}))\boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y})\boldsymbol{h}(\boldsymbol{y}^{-1})),$$

and from the uniqueness property of Lemma 1 (applied when K is replaced by a field containing $K[[\boldsymbol{y}]]$), we deduce

$$\boldsymbol{h}(\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y})\boldsymbol{h}(\boldsymbol{y}^{-1}));$$

finally, substituting $\boldsymbol{y}^{-1}$ to $\boldsymbol{y}$ in that identity, and then $\boldsymbol{x}\boldsymbol{y}$ to $\boldsymbol{x}$, we obtain

$$\boldsymbol{h}(\boldsymbol{x}\boldsymbol{y}) = \boldsymbol{h}(\boldsymbol{h}(\boldsymbol{x})\boldsymbol{h}(\boldsymbol{y})). \tag{2}$$

For a system $\bar{\boldsymbol{x}} = (\bar{x}_k)_{k\in I-J}$ of indeterminates, let now $\sigma(\bar{\boldsymbol{x}})$ be the system $(\sigma_i(\bar{\boldsymbol{x}}))_{i\in I}$ of power series such that $\sigma_i(\bar{\boldsymbol{x}}) = 0$ for $i \in J$, $\sigma_i(\bar{\boldsymbol{x}}) = \bar{x}_i$ for $i \in I - J$; we claim that the system of power series $\Phi(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}}) = (\Phi_k(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}}))_{k\in I-J}$ such that

$$\sigma(\Phi(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}})) = \boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}}))$$

defines a group law. Indeed, it is immediate that $\Phi(\bar{\boldsymbol{e}},\bar{\boldsymbol{x}}) = \Phi(\bar{\boldsymbol{x}},\bar{\boldsymbol{e}}) = \bar{\boldsymbol{x}}$, and from the definitions and from (2), we deduce that

$$\begin{aligned}\sigma(\Phi(\Phi(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}}),\bar{\boldsymbol{z}})) &= \boldsymbol{h}(\sigma(\Phi(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}}))\sigma(\bar{\boldsymbol{z}})) = \boldsymbol{h}(\boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}}))\boldsymbol{h}(\sigma(\bar{\boldsymbol{z}})))\\ &= \boldsymbol{h}(\sigma(\bar{\boldsymbol{x}})\sigma(\bar{\boldsymbol{y}})\sigma(\bar{\boldsymbol{z}})),\end{aligned}$$

and a similar computation for $\sigma(\Phi(\bar{\boldsymbol{x}},\Phi(\bar{\boldsymbol{y}},\bar{\boldsymbol{z}})))$ proves the associativity condition. We will denote by G/H that formal Lie group and we will say that σ is the "typical" cross section of G/H; the system $\bar{\boldsymbol{h}}(\boldsymbol{x})=(h_i(\boldsymbol{x}))_{i\in I-J}$ is then a homomorphism of G into G/H (called the natural homomorphism), and it is clear that $\bar{\boldsymbol{h}}\circ\boldsymbol{j}=0$, $\bar{\boldsymbol{h}}(\sigma(\bar{\boldsymbol{x}}))=\bar{\boldsymbol{x}}$, and $\sigma(\bar{\boldsymbol{h}}(\boldsymbol{x}))=\boldsymbol{h}(\boldsymbol{x})$.

We may now define what we mean by an *exact sequence* of formal Lie groups and homomorphisms of the type

$$0\rightarrow G'\xrightarrow{\boldsymbol{u}}G\xrightarrow{\boldsymbol{v}}G''\rightarrow 0.$$

By definition, this means that there exist a formal Lie group G_1, a typical normal subgroup H_1 of G_1, and three isomorphisms $G'\rightarrow H_1$, $G\rightarrow G_1$, $G''\rightarrow G_1/H_1$, such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & G' \arrow[r, "\boldsymbol{u}"] \arrow[d] & G \arrow[r, "\boldsymbol{v}"] \arrow[d] & G'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H_1 \arrow[r, "\boldsymbol{j}"'] & G_1 \arrow[r, "\bar{\boldsymbol{h}}"'] & G_1/H_1 \arrow[r] & 0
\end{tikzcd}$$

is commutative.

To go further, we should need the homomorphism theorem for formal Lie groups of arbitrary dimension; I do not know if such a theorem is valid in general. However, it will be enough, for our purposes, to consider homomorphisms $\boldsymbol{u}\colon G\rightarrow G'$ of a group G of *finite* dimension into an arbitrary formal Lie group G'. The proof of the homomorphism theorem given in [4, pp. 107-114] can then be transcribed *verbatim,* for all the "changes of variables" which intervene in that proof are defined by power series in the restricted sense which we have adopted at the beginning of this section. There exists therefore (when K is perfect) an isomorphism $G'\rightarrow G_1'$, and an isogeny $G\rightarrow H_1$ of G onto a typical subgroup of G_1', such that the diagram

$$\begin{tikzcd}
G \arrow[r, "\boldsymbol{u}"] \arrow[d] & G' \arrow[d] \\
H_1 \arrow[r, "\boldsymbol{j}"'] & G_1'
\end{tikzcd}$$

is commutative.

3. Cohomology of formal Lie groups. We consider, on one hand, a formal Lie group G of *finite* dimension n over a perfect field K, and on the other hand, an *abelian* formal Lie group A over K, of arbitrary dimension; let I be the finite, J the arbitrary set of indices through which run the indices of the indeterminates defining the group laws of G and A respectively. A structure of *formal G-module* on A is defined by a system $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x})=(f_j(\boldsymbol{s},\boldsymbol{x}))_{j\in J}$ of formal power series without constant terms and with coefficients in K, in the indeterminates s_i and x_j (with $\boldsymbol{s}=(s_i)$, $\boldsymbol{x}=(x_j)$, $i\in I$, $j\in J$); we write $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x})=\boldsymbol{s}\cdot\boldsymbol{x}$, and we assume the following axioms:

$$\boldsymbol{s}\cdot(\boldsymbol{x}+\boldsymbol{y})=\boldsymbol{s}\cdot\boldsymbol{x}+\boldsymbol{s}\cdot\boldsymbol{y} \tag{3}$$

($\boldsymbol{x},\boldsymbol{y}$ independent "generic points" of A, the group A being written additively; if $\boldsymbol{x}+\boldsymbol{y}=(\psi_j(\boldsymbol{x},\boldsymbol{y}))$ is the group law of A, (3), written in full, is the system of identities

$$f_j((s_i),(\psi_k(\boldsymbol{x},\boldsymbol{y})))=\psi_j(\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x}),\boldsymbol{f}(\boldsymbol{s},\boldsymbol{y}));$$

$$\boldsymbol{e}\cdot\boldsymbol{x}=\boldsymbol{x} \tag{4}$$

($\boldsymbol{e}=(0,\cdots,0)$, "neutral element" of G; this means of course that when the s_i are replaced by 0 in each f_j, the resulting series reduces to x_j);

$$\boldsymbol{s}\cdot(\boldsymbol{t}\cdot\boldsymbol{x})=(\boldsymbol{st})\cdot\boldsymbol{x} \tag{5}$$

($\boldsymbol{s},\boldsymbol{t}$ independent "generic points" of G; this means here

$$f_j((s_i),(f_k(\boldsymbol{t},\boldsymbol{x})))=f_j((\phi_i(\boldsymbol{s},\boldsymbol{t})),(x_k))$$

if $\boldsymbol{st}=(\phi_i(\boldsymbol{s},\boldsymbol{t}))$ is the group law of G). The usual properties of modules with coefficients in a group are "formalized" by following the same reasoning as in the classical case: for instance, if L is a field containing $K[[\boldsymbol{s}]]$, condition (3) means that $\boldsymbol{f}(\boldsymbol{s},\boldsymbol{x})$ is an endomorphism of the group $A_{(L)}$, and it follows from (4) and (5) that in fact it is an *automorphism* of that formal Lie group.

For each integer $m\geqq 1$, we now define a (non homogeneous) *m-cochain on G with values in A* as a system $\boldsymbol{g}(\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)=(g_j(\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m))_{j\in J}$ of power series without constant terms and with coefficients in K, in m systems $\boldsymbol{s}_h=(s_{hi})_{i\in I}$ of n indeterminates $(1\leqq h\leqq m)$. We define the "sum" $\boldsymbol{g}+\boldsymbol{h}$ of two m-cochains $\boldsymbol{g}=(g_j)$, $\boldsymbol{h}=(h_j)$ as the system of power series in the s_{hi} obtained by substituting each g_j (resp. h_j) to x_j (resp. y_j) in each of the power series $\psi_j(\boldsymbol{x},\boldsymbol{y})$ defining the group law of A. It is then clear that for that "sum," the m-cochains on G with values in A form a (non formal) abelian group $C^m(G,A)$. We next define the *coboundary operator* $d_{m+1}\colon C^m(G,A)\rightarrow C^{m+1}(G,A)$ by the usual formula

$$\begin{aligned}(6)\qquad d_{m+1}\mathbf{g}(\mathbf{s}_1,\cdots,\mathbf{s}_{m+1}) &= \mathbf{s}_1\cdot\mathbf{g}(\mathbf{s}_2,\cdots,\mathbf{s}_{m+1})\\ &+\sum_{i=1}^{m}(-1)^i\mathbf{g}(\mathbf{s}_1,\cdots,\mathbf{s}_{i-1},\mathbf{s}_i\mathbf{s}_{i+1},\mathbf{s}_{i+2},\cdots,\mathbf{s}_{m+1})\\ &+(-1)^{m+1}\mathbf{g}(\mathbf{s}_1,\cdots,\mathbf{s}_m)\end{aligned}$$

(the sum in the right hand side being taken according to the group law of A; and similarly, the minus signs denote inverses in A); the relation $d_{m+2}d_{m+1}=0$, being purely formal, holds as in the classical case; the subgroup $Z^m(G,A)\subset C^m(G,A)$ of the *m-cocycles* is defined in the usual way for $m\geqq 1$, and the subgroup $B^m(G,A)\subset Z^m(G,A)$ of the *m-coboundaries* for $m\geqq 2$; hence the definition of the *m-th cohomology group*

$$H^m(G,A)=Z^m(G,A)/B^m(G,A)$$

for $m\geqq 2$. As there are no "elements" in A, there is no general definition of $B^1(G,A)$; however, when G operates *trivially* on A, i. e. when $\mathbf{s}\cdot\mathbf{x}=\mathbf{x}$, we take, by definition, $B^1(G,A)=0$, and then it is clear that $H^1(G,A)=Z^1(G,A)$ is the group of *homomorphisms* of G into A.

Let B be a second formal G-module, and $\mathbf{u}=(u_k)$ a *homomorphism* of A into B, i. e. a homomorphism of the abelian group A into the abelian group B such that $\mathbf{u}(\mathbf{s}\cdot\mathbf{x})=\mathbf{s}\cdot\mathbf{u}(\mathbf{x})$; for each m-cochain $\mathbf{g}\in C^m(G,A)$, the system

$$(\mathbf{u}\circ\mathbf{g})(\mathbf{s}_1,\cdots,\mathbf{s}_m)=(u_k(\mathbf{g}(\mathbf{s}_1,\cdots,\mathbf{s}_m)))$$

of power series is an m-cochain $\mathbf{u}\circ\mathbf{g}\in C^m(G,B)$; due to (6) and to the relation $\mathbf{u}(\mathbf{s}\cdot\mathbf{x})=\mathbf{s}\cdot\mathbf{u}(\mathbf{x})$, it is immediately verified that $\mathbf{u}\circ\mathbf{g}$ is a cocycle (resp. a coboundary) when $\mathbf{g}$ is a cocycle (resp. a coboundary). Hence the mapping $u\colon\mathbf{g}\rightarrow\mathbf{u}\circ\mathbf{g}$ defines a homomorphism u^* of $H^m(G,A)$ into $H^m(G,B)$ for $m\geqq 2$ (and also for $m=1$ when G acts trivially on A and on B). Furthermore, it is obvious from the definitions that if C is a third formal G-module, $\mathbf{v}$ a homomorphism of B into C, and $\mathbf{w}=\mathbf{v}\circ\mathbf{u}$, we have for the corresponding homomorphisms, $w^*=v^*\circ u^*$. This implies, in particular, that when A and B are isomorphic formal G-modules, $H^m(G,A)$ and $H^m(G,B)$ are isomorphic.

Consider now a G-module B, and a typical subgroup A of B, corresponding to a subset L of the set J of indices corresponding to B. We say that A is a *submodule* of B if A is a G-module and if, for the natural injection $\mathbf{j}$ of A into B, we have $\mathbf{j}(\mathbf{s}\cdot\mathbf{y})=\mathbf{s}\cdot\mathbf{j}(\mathbf{y})$ ($\mathbf{y}$ generic point of A).

It is then possible to define on B/A a structure of G-module in the following way: with the notations of Section 2 (except that the group law of B is now written additively), we have

$$\begin{aligned} \boldsymbol{s}\cdot\boldsymbol{x} &= \boldsymbol{s}\cdot(\boldsymbol{j}(\boldsymbol{r}(\boldsymbol{x}))) + \boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x}) \\ &= \boldsymbol{j}(\boldsymbol{s}\cdot\boldsymbol{r}(\boldsymbol{x})) + \boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x}) \\ &= \boldsymbol{j}(\boldsymbol{v}(\boldsymbol{x})) + \boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x})), \end{aligned}$$

where $\boldsymbol{v}$ is some system of power series; the uniqueness property of Lemma 1 implies

$$\boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{s}\cdot\boldsymbol{h}(\boldsymbol{x})). \tag{7}$$

It is then an easy matter to verify, using (7) and (2) and the definition of the group law in B/A, that, if we define $\boldsymbol{s}\cdot\bar{\boldsymbol{x}}$ as the system of power series such that $\sigma(\boldsymbol{s}\cdot\bar{\boldsymbol{x}}) = \boldsymbol{h}(\boldsymbol{s}\cdot\sigma(\bar{\boldsymbol{x}}))$, the axioms (3) to (5) are satisfied, and that the natural homomorphism $\bar{\boldsymbol{h}}$ of B onto B/A is a homomorphism of G-modules.

We then extend the definition of an *exact sequence* of G-modules

$$0 \rightarrow A \xrightarrow{\boldsymbol{i}} B \xrightarrow{\boldsymbol{p}} C \rightarrow 0$$

by requesting that, in the corresponding definition given in Section 2 for groups, all the groups are G-modules and all homomorphisms are homomorphisms of G-modules.[2] With that definition, we can verify immediately that the corresponding sequence of (non formal) abelian groups and homomorphisms

$$0 \rightarrow C^m(G,A) \xrightarrow{i} C^m(G,B) \xrightarrow{p} C^m(G,C) \rightarrow 0$$

is *exact*: we can namely suppose first that A is a typical submodule of B, C the quotient module B/A, and that $\boldsymbol{i}$ and $\boldsymbol{p}$ are the natural homomorphisms $\boldsymbol{j}$ and $\bar{\boldsymbol{h}}$. Suppose that $\boldsymbol{g}$ is an m-cochain in $C^m(G,B)$ such that $\bar{\boldsymbol{h}}\circ\boldsymbol{g} = 0$; using Lemma 1, we can write

$$\boldsymbol{g} = \boldsymbol{j}\circ\boldsymbol{g}_1 + \sigma\circ\boldsymbol{g}_2,$$

where $\boldsymbol{g}_1 \in C^m(G,A)$ and $\boldsymbol{g}_2 \in C^m(G,B)$; the assumption means that $\sigma\circ\boldsymbol{g}_2 = 0$, hence our conclusion.

The general methods of cohomology can then be applied to define homomorphisms $\partial: H^m(G,C) \to H^{m+1}(G,A)$ for $m \geqq 2$, and to prove that the sequence

---

[2] The field K has here arbitrary characteristic, and there can be no confusion between the meaning of the letter $\boldsymbol{p}$ here and its usual meaning (Frobenius homomorphism) in groups over a field of characteristic p.

$$(8)\quad H^2(G,A) \xrightarrow{i^*} H^2(G,B) \xrightarrow{p^*} H^2(G,C) \xrightarrow{\partial} H^3(G,A) \to \cdots$$

$$\cdots \to H^m(G,A) \xrightarrow{i^*} H^m(G,B) \xrightarrow{p^*} H^m(G,C) \xrightarrow{\partial} H^{m+1}(G,A) \to \cdots$$

is *exact* ("exact sequence of cohomology"); furthermore, when G operates trivially on A, B and C, the sequence can begin with $H^1(G,A)$, as is readily verified. Finally, suppose we have two exact sequence of G-modules, connected by homomorphisms

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "u"'] & B \arrow[r] \arrow[d, "v"'] & C \arrow[r] \arrow[d, "w"'] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

such that the diagram is commutative; it is then clear that the corresponding diagram for m-cochains

$$\begin{tikzcd}
0 \arrow[r] & C^m(G,A) \arrow[r] \arrow[d, "u"'] & C^m(G,B) \arrow[r] \arrow[d, "v"'] & C^m(G,C) \arrow[r] \arrow[d, "w"'] & 0 \\
0 \arrow[r] & C^m(G,A') \arrow[r] & C^m(G,B') \arrow[r] & C^m(G,C') \arrow[r] & 0
\end{tikzcd}$$

is commutative, and then the general methods of cohomology prove that the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & H^m(G,A) \arrow[r] \arrow[d, "u^*"'] & H^m(G,B) \arrow[r] \arrow[d, "v^*"'] & H^m(G,C) \arrow[r] \arrow[d, "w^*"'] & H^{m+1}(G,A) \arrow[r] \arrow[d, "u^*"'] & \cdots \\
\cdots \arrow[r] & H^m(G,A') \arrow[r] & H^m(G,B') \arrow[r] & H^m(G,C') \arrow[r] & H^{m+1}(G,A') \arrow[r] & \cdots
\end{tikzcd}$$

is also commutative.

4. The Hochschild-Serre exact sequence.[3]

Let u be a homomorphism of a formal Lie group H (of finite dimension) into G. It is immediate that, if A is a G-module, A is made into an H-module if we define $\boldsymbol{t} \cdot \boldsymbol{x}$ as equal to $\boldsymbol{u}(\boldsymbol{t}) \cdot x$ for a "generic point" $\boldsymbol{t}$ of H. If $\boldsymbol{g}$ is any cochain in $C^m(G, A)$, then $\boldsymbol{g}'(\boldsymbol{t}_1, \cdots, \boldsymbol{t}_m) = \boldsymbol{g}(\boldsymbol{u}(\boldsymbol{t}_1), \cdots, \boldsymbol{u}(\boldsymbol{t}_m))$ is an m-cochain in $C^m(H, A)$; if we denote it by $\bar{u}(\boldsymbol{g})$, $\bar{u}$ is a homomorphism of $C^m(G, A)$ into $C^m(H, A)$, and formula (6) shows that $\bar{u}$ commutes with d_{m+1}. Hence, for $m \geqq 2$, we have a homomorphism

---

[3] The result which we prove in this section is the extension to our situation of a very special corollary of the results of Hochschild and Serre [11]; they use very heavy homological machinery, and the labor of extending that machinery to the present case would (if possible at all) be out of proportion to our needs. The "elementary" proof which I follow here is patterned after a similar proof for the classical case, which was kindly communicated to me by G. Hochschild.

$$u^* : H^m(G, A) \rightarrow H^m(H, A);$$

when G operates trivially on A, so does H, and the definition of u^* can be extended for $m = 1$. Furthermore, it is readily verified that, for any exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ of G-modules, the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & H^m(G,A) \arrow[r] \arrow[d, "u^*"'] & H^m(G,B) \arrow[r] \arrow[d, "u^*"'] & H^m(G,C) \arrow[r] \arrow[d, "u^*"'] & H^{m+1}(G,A) \arrow[r] \arrow[d, "u^*"'] & \cdots \\
\cdots \arrow[r] & H^m(H,A) \arrow[r] & H^m(H,B) \arrow[r] & H^m(H,C) \arrow[r] & H^{m+1}(H,A) \arrow[r] & \cdots
\end{tikzcd}$$

is commutative.

From now on, we shall suppose that the G-module A has *finite* dimension. We introduce, after A. Weil (cf. [11, p. 114, Cor. to Prop. 3]), a new formal abelian group $M(G, A)$ of infinite dimension, corresponding to the set of indices $L = J \times \boldsymbol{N}^I$; for two "generic points" $\boldsymbol{u} = (u_{j\alpha})$, $\boldsymbol{v} = (v_{j\alpha})$, the composition law $\boldsymbol{w} = \boldsymbol{u} + \boldsymbol{v}$ is defined in the following way. We associate to $\boldsymbol{u}$ and to a "generic point" $\boldsymbol{s}$ of G the system of power series which we write $\boldsymbol{u}(\boldsymbol{s}) = (u_j(\boldsymbol{s}))$ in the $u_{j\alpha}$ and s_i, such that $u_j(\boldsymbol{s}) = \sum_{\alpha} u_{j\alpha} \boldsymbol{s}^\alpha$ (note that these series have no constant term, but each one has a unique term which does not contain any s_i, namely u_{j0}); the mapping $\boldsymbol{u} \rightarrow \boldsymbol{u}(\boldsymbol{s})$ is of course bijective; $\boldsymbol{w}$ is then defined by the condition $\boldsymbol{w}(\boldsymbol{s}) = \boldsymbol{u}(\boldsymbol{s}) + \boldsymbol{v}(\boldsymbol{s})$ (sum taken for the group law of A), and it is immediately verified that $w_{j\alpha}$ is actually a *polynomial* in the $u_{j\alpha}$ and $v_{j\alpha}$; the associativity and commutativity of the group law are obvious. We next make $M(G, A)$ into a G-module by the definition $(\boldsymbol{s} \cdot \boldsymbol{u})(\boldsymbol{s}') = \boldsymbol{u}(\boldsymbol{s}'\boldsymbol{s})$ ($\boldsymbol{s}, \boldsymbol{s}'$ independent generic points of G); if we write as usual $(\boldsymbol{s}'\boldsymbol{s})^\gamma = \sum_{\alpha,\beta} d_{\alpha\beta\gamma} \boldsymbol{s}'^\alpha \boldsymbol{s}^\beta$, we have therefore, for $\boldsymbol{v} = \boldsymbol{s} \cdot \boldsymbol{u}$, $v_{j\alpha} = \sum_{\beta,\gamma} d_{\alpha\beta\gamma} u_{j\gamma} \boldsymbol{s}^\beta$, and as G has finite dimension, there are only a finite number of $d_{\alpha\beta\gamma}$ which are $\neq 0$ for given α and β, which shows that the power series defining $\boldsymbol{s} \cdot \boldsymbol{u}$ are of the type allowed by our conventions; the verification of axioms (3), (4) and (5) is then immediate. Observe in passing that for the definition of the structure of G-module on $M(G, A)$, the structure of G-module of A is irrelevant, only its structure of abelian group intervenes.

It is immediate from the definitions that for any m-cochain $\boldsymbol{f}$ in $C^m(G,M)$, $\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)=\boldsymbol{f}(\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)(\boldsymbol{s}_0)$ is an $(m+1)$-cochain in $C^{m+1}(G,A)$, and $\boldsymbol{f}\rightarrow\boldsymbol{f}_*$ is an isomorphism of $C^m(G,M)$ onto $C^{m+1}(G,A)$. Moreover, we can here define 1-coboundaries in $C^1(G,M)$ as the 1-cochains $\boldsymbol{f}$ such that $\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1)=\boldsymbol{g}(\boldsymbol{s}_0\boldsymbol{s}_1)-\boldsymbol{g}(\boldsymbol{s}_0)$, where $\boldsymbol{g}$ is a 1-cochain in $C^1(G,A)$. For any subgroup H of G, $M(G,A)$ is also an H-module, and the cochains in $C^m(H,M)$ correspond now to the systems of power series $\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)$, where $\boldsymbol{s}_0$ is a generic point of G, $\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m$ independent generic points *of* H; 1-coboundaries are again defined in the same way. With these definitions:

LEMMA 2. *For any subgroup H of G, $H^m(H,M(G,A))=0$ for any $m\geqq 1$.*

Indeed, if we write that an m-cochain $\boldsymbol{f}\in C^m(H,M)$ is such that $d_{m+1}\boldsymbol{f}=0$, we obtain, from formula (6)

$$\boldsymbol{f}_*(\boldsymbol{s}_0\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_{m+1})+\sum_{i=1}^{m}(-1)^i\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_i\boldsymbol{s}_{i+1},\cdots,\boldsymbol{s}_{m+1}) + (-1)^{m+1}\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)=0. \tag{9}$$

when $\boldsymbol{s}_0$ is a generic point of G, the $\boldsymbol{s}_i$ $(i\geqq 1)$ independent generic points of H. We may obviously suppose the subgroup H is typical, defined, for instance, by the relations $s_i=0$ for $i\in I-I_0$. Using Lemma 1, we can therefore write for a generic point $\boldsymbol{s}$ of G, $\boldsymbol{s}=\boldsymbol{h}(\boldsymbol{s})\boldsymbol{r}(\boldsymbol{s})$, where $h_i(\boldsymbol{s})=0$ for $i\in I_0$, $r_i(\boldsymbol{s})=0$ for $i\in I-I_0$; if $\boldsymbol{t}$ is a generic point of H, we have $\boldsymbol{h}(\boldsymbol{t})=\boldsymbol{e}$, $\boldsymbol{r}(\boldsymbol{t})=\boldsymbol{t}$; using these results and the uniqueness property of Lemma 1, it is easy to verify, as in Section 2, that $\boldsymbol{h}(\boldsymbol{st})=\boldsymbol{h}(\boldsymbol{s})$ and $\boldsymbol{r}(\boldsymbol{st})=\boldsymbol{r}(\boldsymbol{s})\boldsymbol{t}$. Consider now the system of power series

$$\boldsymbol{g}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_{m-1})=\boldsymbol{f}_*(\boldsymbol{h}(\boldsymbol{s}_0),\boldsymbol{r}(\boldsymbol{s}_0),\boldsymbol{s}_1,\cdots,\boldsymbol{s}_{m-1})$$

with the same assumptions on the $\boldsymbol{s}_i$; formula (9) and the preceding properties of $\boldsymbol{h}$ and $\boldsymbol{r}$ show at once that $\boldsymbol{f}=d_m\boldsymbol{g}$, hence our result (the case $m=1$ has, of course, to be considered separately, since we have not defined 0-cochains, but directly 1-coboundaries).

We next introduce the *lift* mapping. Let P be a G-module (of finite or infinite dimension), and let H be a *normal* subgroup of G; suppose in addition that the relations $\boldsymbol{t}\cdot\boldsymbol{x}=\boldsymbol{x}$, for a generic point $\boldsymbol{t}$ of H, "define" a subgroup P^H of P (this means that, after a suitable "change of variables" in P, the equations obtained by writing that in the power series $f_j(\boldsymbol{t},\boldsymbol{x})$, considered as series in the t_i, the coefficients are all zero except the terms independent of $\boldsymbol{t}$, form a system equivalent to the system obtained by equating to 0 a subset of the indeterminates x_j). Then, if $\boldsymbol{y}$ is a generic point of P^H, we have $(\boldsymbol{ts})\cdot\boldsymbol{y}=\boldsymbol{s}\cdot\boldsymbol{y}$ for a generic point $\boldsymbol{s}$ of G, since H is normal in G; therefore P^H is a G-submodule. We may suppose that H is a typical normal subgroup of G, and keep the notations of Lemma 2. For a system of indeterminates $\bar{\boldsymbol{s}}=(\bar{s}_k)_{k\in I-I_0}$, we define $\sigma(\bar{\boldsymbol{s}})=(\sigma_i(\bar{\boldsymbol{s}}))$ such that $\sigma_i(\bar{\boldsymbol{s}})=0$ for $i\in I_0$, $\sigma_i(\bar{\boldsymbol{s}})=\bar{s}_i$ for $i\in I-I_0$; it is readily verified that $\bar{\boldsymbol{s}}\cdot\boldsymbol{y}=\sigma(\bar{\boldsymbol{s}})\cdot\boldsymbol{y}$ defines a structure of (G/H)-module on P^H, and that the original structure of G-module on P^H is obtained by the process described at the beginning of this section applied to the natural homomorphism $\bar{\boldsymbol{h}}$ of G into G/H. If we designate by $\boldsymbol{i}$ the natural injection $P^H\rightarrow P$, we obtain therefore a homomorphism

$$\lambda\colon H^m(G/H,P^H)\xrightarrow{\bar{h}^*}H^m(G,P^H)\xrightarrow{i^*}H^m(G,P)$$

$(m\geqq 2)$, which we call the *lift* mapping.

It can also be described as deriving (by passage to quotients) from the mapping

$$\lambda\colon C^m(G/H,P^H)\rightarrow C^m(G,P)$$

which to each cochain $\boldsymbol{g}(\bar{\boldsymbol{s}}_1,\cdots,\bar{\boldsymbol{s}}_m)$ in $C^m(G/H,P^H)$, associates the cochain $\boldsymbol{i}(\boldsymbol{g}(\bar{\boldsymbol{h}}(\boldsymbol{s}_1),\cdots,\bar{\boldsymbol{h}}(\boldsymbol{s}_m)))$ in $C^m(G,P)$.

We can now state and prove the main result of this section:

PROPOSITION 1. *Suppose A is an abelian Lie group of finite dimension, on which G operates trivially, and that H is a normal subgroup of G such that $H^1(H_{(N)},A_{(N)})=0$ for any extension N of the field K. Then the sequence*

$$0\rightarrow H^2(G/H,A)\xrightarrow{\lambda^*}H^2(G,A)\xrightarrow{\rho^*}H^2(H,A)$$

(ρ natural injection of H into G) is exact.

We introduce, as above, the G-module $M(G,A)=M$, and we consider in addition the mapping $\boldsymbol{j}\colon A\rightarrow M$ such that $j_{k0}(\boldsymbol{x})=x_k$, $j_{k\alpha}(\boldsymbol{x})=0$ whenever $\alpha\neq 0$ $(k\in J)$ (in other words, $\boldsymbol{j}(\boldsymbol{x})(\boldsymbol{s})=(j_k(\boldsymbol{x},\boldsymbol{s}))$ is the system of power series $j_k(\boldsymbol{x},\boldsymbol{s})=x_k$). As G operates trivially on A, $\boldsymbol{j}$ is a homomorphism of G-modules; homeover $\boldsymbol{j}(A)$ is the typical subgroup of M defined by the relations $u_{k\alpha}=0$ for $\alpha\in J$ and $\alpha\neq 0$. We may therefore consider the quotient G-module $C=M/\boldsymbol{j}(A)$; we shall denote by $\boldsymbol{p}$ the natural homomorphism of M into C; we have by definition $\boldsymbol{s}\cdot\boldsymbol{p}(\boldsymbol{u})=\boldsymbol{p}(\boldsymbol{s}\cdot\boldsymbol{u})$.

From that definition, it follows that for any m-cochain $\boldsymbol{f}$ in $C^m(G,C)$, $\tau(\boldsymbol{f}(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_m))(\boldsymbol{s}_0)=\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m)$ (τ typical cross section of $M/\boldsymbol{j}(A)$) is a system of power series in which there are no terms independent of $\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m$, i.e. such that $\boldsymbol{f}_*(\boldsymbol{s}_0,\boldsymbol{e},\cdots,\boldsymbol{e})=0$. We observe that the 1-coboundaries in $C^1(G,M)$, as defined above, have that property, and by definition, we take these 1-cochains as 1-coboundaries in $C^1(G,C)$; the cochains in $C^m(H,C)$ and the 1-coboundaries in $C^1(H,C)$ are characterized in the same way.

We now proceed to show that M^H and C^H are "defined" in the sense described above, and to characterize these submodules. The relation $\boldsymbol{t}\cdot\boldsymbol{u}=\boldsymbol{u}$ means $\boldsymbol{u}(\boldsymbol{st})=\boldsymbol{u}(\boldsymbol{s})$ ($\boldsymbol{s}$ generic point of G, $\boldsymbol{t}$ generic point of H); using the notations introduced in Lemma 2, this implies $\boldsymbol{u}(\boldsymbol{s})=\boldsymbol{u}(\boldsymbol{h}(\boldsymbol{s})\boldsymbol{r}(\boldsymbol{s}))=\boldsymbol{u}(\boldsymbol{h}(\boldsymbol{s}))$; conversely, for any system $\boldsymbol{v}=(v_{k\alpha})$ of indeterminates, $\boldsymbol{u}(\boldsymbol{s})=\boldsymbol{v}(\boldsymbol{h}(\boldsymbol{s}))$ is such that $\boldsymbol{u}(\boldsymbol{st})=\boldsymbol{u}(\boldsymbol{s})$. If we remember that $h_i(\boldsymbol{s})=0$ for $i\in I_0$, $h_i(\boldsymbol{s})=s_i+\cdots$ (unwritten terms of degree $\geqq 2$) for $i\in I-I_0$, it follows easily, by induction on $|\alpha|$, that the relation $\boldsymbol{t}\cdot\boldsymbol{u}=\boldsymbol{u}$ is equivalent to an infinite system of equations of the following type: $u_{k,\epsilon_i}=0$ for $i\in I_0$, and, for any index $\alpha=(\alpha_1,\cdots,\alpha_n)$ such that $|\alpha|>1$ and one at least of the α_i for $i\in I_0$ is $\neq 0$,

$$u_{k\alpha}=P_{k\alpha}((u_{j\beta})) \qquad (k\in J),$$

where $P_{k\alpha}$ is a polynomial with integral coefficients in the $u_{j\beta}$ $(j\in J)$ such that $|\beta|<|\alpha|$ and all non-zero components of β have their index in $I-I_0$. The "change of variables" $u'_{k\alpha}=u_{k\alpha}-P_{k\alpha}((u_{j\beta}))$ for all indices α such that at least one α_i for $i\in I_0$ is $\neq 0$ (with $P_{k\alpha}=0$ if $|\alpha|=1$) reduces M^H to a typical subgroup. This shows further that the mapping $\boldsymbol{v}\rightarrow\boldsymbol{v}\circ\bar{\boldsymbol{h}}$ is an isomorphism of the abelian group $M(G/H,A)$ onto M^H; moreover, if $\bar{\boldsymbol{s}}'$ is a generic point of G/H, we have

$$\begin{aligned}(\bar{\boldsymbol{s}}'\cdot\boldsymbol{v})(\bar{\boldsymbol{h}}(\boldsymbol{s}))&=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s})\bar{\boldsymbol{s}}')=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s})\bar{\boldsymbol{h}}(\sigma(\bar{\boldsymbol{s}}')))\\&=\boldsymbol{v}(\bar{\boldsymbol{h}}(\boldsymbol{s}\sigma(\bar{\boldsymbol{s}}')))=(\sigma(\bar{\boldsymbol{s}}')\cdot(\boldsymbol{v}\circ\bar{\boldsymbol{h}}))(\boldsymbol{s})\end{aligned}$$

which proves that the preceding isomorphism is also an isomorphism of (G/H)-modules. We deduce therefore from Lemma 2 that $H^m(G/H,M^H)=0$ for any $m\geqq 1$.

Our next step is to prove that, due to the relation $H^1(H_{(N)},A_{(N)})=0$, the sequence $0\rightarrow A\xrightarrow{\boldsymbol{j}}M^H\xrightarrow{\boldsymbol{p}^H}C^H\rightarrow 0$ (where $\boldsymbol{p}^H$ is the restriction of $\boldsymbol{p}$ to M^H) is *exact*. If $\bar{\boldsymbol{u}}$ is a generic point of C, the condition $\boldsymbol{t}\cdot\bar{\boldsymbol{u}}=\bar{\boldsymbol{u}}$ which defines C^H is equivalent to $\boldsymbol{p}(\boldsymbol{t}\cdot\tau(\bar{\boldsymbol{u}})-\tau(\bar{\boldsymbol{u}}))=0$; the components of $\tau(\bar{\boldsymbol{u}})$

are $\tau_{k0}(\bar{\boldsymbol{u}}) = 0$ for $k \in J$ and $\tau_{k\alpha}(\bar{\boldsymbol{u}}) = \bar{u}_{k\alpha}$ for $\alpha \neq 0$, $k \in J$; if we write $\boldsymbol{w} = \tau(\bar{\boldsymbol{u}})$ for simplicity's sake, the relation $\boldsymbol{t} \cdot \bar{\boldsymbol{u}} = \bar{\boldsymbol{u}}$ means that the power series of the system $\boldsymbol{w}(\boldsymbol{st}) - \boldsymbol{w}(\boldsymbol{s})$ (considered as power series in the s_i) have all their coefficients 0 except the constant terms (which are power series in the t_i $(i \in I_0)$ and the $\bar{u}_{k\alpha}$); as $\boldsymbol{w}(\boldsymbol{e}) = 0$, we have therefore

$$\boldsymbol{w}(\boldsymbol{st}) - \boldsymbol{w}(\boldsymbol{s}) = \boldsymbol{w}(\boldsymbol{t}).$$

From this relation it follows, in particular, if $\boldsymbol{t}'$ is a second generic point of H, that $\boldsymbol{w}(\boldsymbol{t}'\boldsymbol{t}) = \boldsymbol{w}(\boldsymbol{t}') + \boldsymbol{w}(\boldsymbol{t})$; if N is a field containing $K[[\bar{\boldsymbol{u}}]]$, this means that the system of power series $\boldsymbol{w}(\boldsymbol{t})$ over N is a homomorphism of $H_{(N)}$ into $A_{(N)}$. Our assumption implies that $\boldsymbol{w}(\boldsymbol{t}) = 0$, hence $\boldsymbol{w}(\boldsymbol{st}) = \boldsymbol{w}(\boldsymbol{s})$; in other words, the relation $\boldsymbol{t} \cdot \bar{\boldsymbol{u}} = \bar{\boldsymbol{u}}$ implies that $\tau(\bar{\boldsymbol{u}})$ verifies the condition which defines M^H, and the converse is obvious, which proves our assertion.

We may observe here that the relations $u_{k0} = 0$ $(k \in J)$ also define a subgroup in M, and τ is an isomorphism of C onto that subgroup; similarly, when M^H is identified with $M(G/H, A)$, τ, restricted to C^H, is an isomorphism of that group onto the subgroup of $M(G/H, A)$ defined in a similar way. In particular, we see that the 1-cochains in $C^1(G/H, C^H)$ are identified to systems $\boldsymbol{f}_*(\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{s}}_1)$ ($\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{s}}_1$ independent generic points in G/H) such that $\boldsymbol{f}_*(\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{e}}) = 0$, and the 1-coboundaries in $C^1(G/H, C^H)$ can again be identified with the 1-coboundaries in $C^1(G/H, M^H)$. The 1-coboundaries in $C^1(G, C)$ (resp. $C^1(G/H. C^H)$) are thus the images by p (resp. p^H) of the 1-coboundaries in $C(G, M)$ (resp. $C^1(G/H, M^H)$). It is then a routine matter to verify that these remarks allow us to define the homomorphisms ∂ in the horizontal lines of the following diagram, and to prove that these lines are exact sequences:

(10)

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & \\
0 = H^1(G/H, M^H) \arrow[r] & H^1(G/H, C^H) \arrow[r, "\partial"] \arrow[d, "\lambda^*"] & H^2(G/H, A) \arrow[r] \arrow[d, "\lambda^*"] & H^2(G/H, M^H) = 0 \\
0 = H^1(G, M) \arrow[r] & H^1(G, C) \arrow[r, "\partial"] \arrow[d, "\rho^*"] & H^2(G, A) \arrow[r] \arrow[d, "\rho^*"] & H^2(G, M) = 0 \\
0 = H^1(K, M) \arrow[r] & H^1(K, C) \arrow[r, "\partial"] & H^2(K, A) \arrow[r] & H^2(K, M) = 0
\end{tikzcd}$$

The second vertical line has already been defined, but we still have to define the first vertical line and to prove that the diagram (10) is commutative. If a cochain $\boldsymbol{f}$ in $C^1(G/H, C^H)$ is identified to the system of power series

$f_*(\bar{s}_0, \bar{s}_1)$ (such that $f_*(\bar{s}_0, \bar{e}) = 0$), $\lambda(f)$ is by definition the cochain associated to the system $f_*(\bar{h}(s_0), \bar{h}(s_1))$. From the definitions, it follows that $\lambda(\bar{s} \cdot f)$ is equal to $\sigma(\bar{s}) \cdot \lambda(f)$; hence, if f is a cocycle, so is $\lambda(f)$; furthermore, the definitions given above show that if f is a 1-coboundary, so is $\lambda(f)$, hence the definition of $\lambda^*\colon H^1(G/H, C^H) \to H^1(G, C)$. In addition, if f is a cocycle belonging to the cohomology class c, the class ∂c contains the 2-cocycle $f_*(\bar{s}_0, \bar{s}_1) - f_*(\bar{e}, \bar{s}_0\bar{s}_1) + f_*(\bar{e}, \bar{s}_0)$, as is immediate from the definition of ∂; a similar computation for $\partial(\lambda^*(c))$ proves the commutativity in the two first horizontal lines of the diagram. The definition of ρ^* and the verification of the commutativity in the last two horizontal lines are even simpler and we omit them.

We have used Lemma 2 to replace the left and right extremities of the horizontal lines in (10) by 0; to end the proof of Proposition 1, it remains therefore to prove that the first vertical line is an exact sequence. We first show that λ^* is injective. With the same notations as above, suppose $\lambda(f)$ is a coboundary; this means that $f_*(\bar{h}(s_0), \bar{h}(s_1)) = g(s_0s_1) - g(s_0)$; but if t is a generic point of H, $\bar{h}(s_1t) = \bar{h}(s_1)$, hence $g(s_0s_1t) = g(s_0s_1)$; replacing s_0 by e, s_1 by $h(s)$, t by $r(s)$ (s generic point of G; notations of Lemma 2), we get $g(s) = g(h(s)) = g(\sigma(\bar{h}(s)))$, and therefore f is a coboundary.

Finally, it is clear that $\rho^*\lambda^* = 0$, and we have only to show that any element in the kernel of ρ^* is in the image of λ^*. Let therefore f be a cocycle in $C^1(G, C)$ such that the image by ρ^* of its cohomology class is 0. This means that $f_*(s_0, s_1)$ is such that, for a generic point t of H, $f_*(s_0, t) = g(s_0t) - g(s_0)$. Using equation (9) (for $m = 1$), we get

$$f_*(s_0, s_1t) = f_*(s_0s_1, t) + f_*(s_0, s_1) = f_*(s_0, s_1) + g(s_0s_1t) - g(s_0s_1).$$

Let $f'_*(s_0, s_1) = f_*(s_0, s_1) - g(s_0s_1) + g(s_0)$; then f' is obviously a cocycle which is cohomologous to f, and we have

$$f'_*(s_0, s_1t) = f'_*(s_0, s_1). \tag{11}$$

As $ts_1 = s_1(s_1^{-1}ts_1)$, and H is normal, (11) also implies

$$f'_*(s_0, ts_1) = f'_*(s_0, s_1); \tag{12}$$

on the other hand, equation (9) yields

$$f'_*(s_0t, s_1) - f'_*(s_0, ts_1) + f'_*(s_0, t) = 0,$$

and we have, by assumption, $f'_*(s_0, t) = 0$, hence

$$f'_*(s_0t, s_1) = f'_*(s_0, s_1). \tag{13}$$

Equations (11) and (13) show that, if $\boldsymbol{f}''_*(\bar{\boldsymbol{s}}_0, \bar{\boldsymbol{s}}_1) = \boldsymbol{f}'_*(\sigma(\bar{\boldsymbol{s}}_0), \sigma(\bar{\boldsymbol{s}}_1))$, $\boldsymbol{f}''$ is a cocycle in $C^1(G/H, C^H)$ and that $\boldsymbol{f}' = \lambda \boldsymbol{f}''$); the proof of Proposition 1 is thus complete.

5. Group extensions and cohomology. Let A, B be two formal Lie groups of finite dimension over a perfect field K. We say that a formal Lie group G over K and a pair of homomorphisms $A \xrightarrow{\boldsymbol{u}} G \xrightarrow{\boldsymbol{v}} B$ constitute an *extension of B by A* if $\boldsymbol{u}$ is a monomorphism, $\boldsymbol{v}$ an epimorphism and if the kernel of $\boldsymbol{v}$ is equal to the image of $\boldsymbol{u}$; B is then isomorphic to $G/\boldsymbol{u}(A)$. We say, as usual, that two extensions $(G, \boldsymbol{u}, \boldsymbol{v})$, $(G_1, \boldsymbol{u}_1, \boldsymbol{v}_1)$ are *equivalent* if there exists an isomorphism $\boldsymbol{f}\colon G \to G_1$ such that the diagram

$$\begin{tikzcd}
& G \arrow[dr, "\boldsymbol{v}"] \arrow[dd, "\boldsymbol{f}"] & \\
A \arrow[ur, "\boldsymbol{u}"] \arrow[dr, "\boldsymbol{u}_1"'] & & B \\
& G_1 \arrow[ur, "\boldsymbol{v}_1"'] &
\end{tikzcd}$$

is commutative. If α is an isomorphism of K onto a field K', and if we denote by A^α, B^α, G^α, $\boldsymbol{u}^\alpha$, $\boldsymbol{v}^\alpha$ the groups and homomorphisms obtained by applying to all coefficients of the series defining A, B, G, $\boldsymbol{u}$, $\boldsymbol{v}$ the isomorphism α, it is clear from the definitions that $A^\alpha \xrightarrow{\boldsymbol{u}^\alpha} G^\alpha \xrightarrow{\boldsymbol{v}^\alpha} B^\alpha$ is again an extension.

Suppose $\dim G = n$, $\dim B = m$ (hence $\dim A = n - m$). We say that a system $\sigma(\bar{\boldsymbol{x}}) = (\sigma_k(\bar{\boldsymbol{x}}))_{1 \leqq k \leqq n}$ of power series without constant terms in the $\bar{x}_i$ $(1 \leqq i \leqq m)$ is a *cross-section* for the extension $(G, \boldsymbol{u}, \boldsymbol{v})$ if $\boldsymbol{v}(\sigma(\bar{\boldsymbol{x}})) = \bar{\boldsymbol{x}}$; we have proved in Section 2 the existence of cross-sections for any extension. Then if we write (for a generic point $\boldsymbol{s}$ of G), $\boldsymbol{r}(\boldsymbol{s}) = \boldsymbol{s} \cdot (\sigma(\boldsymbol{v}(\boldsymbol{s})))^{-1}$, it is clear that $\boldsymbol{v}(\boldsymbol{r}(\boldsymbol{s})) = \bar{\boldsymbol{e}}$; hence, we see at once (taking, for instance, the subgroup $\boldsymbol{u}(A)$ of G in typical form) that we can write $\boldsymbol{r}(\boldsymbol{s}) = \boldsymbol{u}(\rho(\boldsymbol{s}))$, where $\rho(\boldsymbol{s})$ is a system $(\rho_j(\boldsymbol{s}))$ $(1 \leqq j \leqq n - m)$ of power series without constant terms. From the relation $\boldsymbol{s} = \boldsymbol{u}(\rho(\boldsymbol{s}))\sigma(\boldsymbol{v}(\boldsymbol{s}))$, it follows at once by considering the jacobians of the systems of power series on both sides, that the power series $t_j = \rho_j(\boldsymbol{s})$ $(1 \leqq j \leqq n - m)$ and $y_k = v_k(\boldsymbol{s})$ $(1 \leqq k \leqq m)$ define a change of variables in G; in other words, considering $\boldsymbol{t} = (t_j)$ as a generic point of A, $\boldsymbol{y} = (y_k)$ as a generic point of B, we can write $\boldsymbol{s} = \boldsymbol{u}(\boldsymbol{t})\sigma(\boldsymbol{y})$.

We will suppose from now on that, unless the contrary is explicitly stated, A is *abelian.* We can then define on A a structure of *B-module,* by defining $\boldsymbol{y}\cdot\boldsymbol{t}'$ ($\boldsymbol{t}'$ second independent generic point of A) such that $\boldsymbol{u}(\boldsymbol{y}\cdot\boldsymbol{t}') = \sigma(\boldsymbol{y})\boldsymbol{u}(\boldsymbol{t}')(\sigma(\boldsymbol{y}))^{-1}$; the verification of axioms (3) and (4) is immediate, and (5) follows from the commutativity of A. On the other hand, we have, for a second independent generic point $\boldsymbol{y}'$ of B, $\boldsymbol{v}(\sigma(\boldsymbol{y})\sigma(\boldsymbol{y}')) = \boldsymbol{y}\boldsymbol{y}'$; hence $\sigma(\boldsymbol{y})\sigma(\boldsymbol{y}') = \boldsymbol{u}(\boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}'))\sigma(\boldsymbol{y}\boldsymbol{y}')$, where $\boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}') = \rho(\sigma(\boldsymbol{y})\sigma(\boldsymbol{y}'))$. Therefore writing A additively, we have

$$\text{(14)} \qquad \boldsymbol{u}(\boldsymbol{t})\sigma(\boldsymbol{y})\boldsymbol{u}(\boldsymbol{t}')\sigma(\boldsymbol{y}') = \boldsymbol{u}(\boldsymbol{t} + \boldsymbol{y}\cdot\boldsymbol{t}' + \boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}'))\sigma(\boldsymbol{y}\boldsymbol{y}').$$

If we write the associativity condition, we find in the usual way that $\boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}')$ is a *2-cocycle* on B with values in A; conversely, given an arbitrary 2-cocycle $\boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}')$, the formal Lie G group defined by the group law

$$\phi((\boldsymbol{t},\boldsymbol{y}),(\boldsymbol{t}',\boldsymbol{y}')) = (\boldsymbol{t} + \boldsymbol{y}\cdot\boldsymbol{t}' + \boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}'),\boldsymbol{y}\boldsymbol{y}')$$

together with the homomorphisms $\boldsymbol{u}\colon \boldsymbol{t}\to(\boldsymbol{t},\boldsymbol{e})$ and $\boldsymbol{v}\colon(\boldsymbol{t},\boldsymbol{y})\to\boldsymbol{y}$ constitute an extension of B by A. Furthermore, if $\sigma'(\tilde{\boldsymbol{x}})$ is a second cross-section, we can write $\sigma'(\boldsymbol{y}) = \boldsymbol{u}(\boldsymbol{c}(\boldsymbol{y}))\sigma(\boldsymbol{y})$, with $\boldsymbol{c}(\boldsymbol{y}) = \rho(\sigma'(\boldsymbol{y}))$, and the 2-cocycle corersponding to σ' is easily computed to be

$$\boldsymbol{a}'(\boldsymbol{y},\boldsymbol{y}') = \boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}') + \boldsymbol{y}\cdot\boldsymbol{c}(\boldsymbol{y}') - \boldsymbol{c}(\boldsymbol{y}\boldsymbol{y}') + \boldsymbol{c}(\boldsymbol{y});$$

in other words, it differs from $\boldsymbol{a}(\boldsymbol{y},\boldsymbol{y}')$ by a 2-coboundary. We thus obtain, as in the classical theory, a one-to-one correspondence between classes of equivalent extensions of B by A, corresponding to the *same* structure of B-module on A, and the second cohomology group $H^2(B,A)$ corresponding to that structure. We can also interpret the extensions corresponding to the trivial cohomology class (so called *trivial extensions*) by the classical notion of *semi-direct product*: we need not here suppose A *commutative* (and we write it multiplicatively); if $\boldsymbol{y}$ is a generic point of B, $\boldsymbol{t}$ a generic point of A, we suppose given a system $\boldsymbol{t}^{\boldsymbol{y}}$ of power series without constant terms in the components of $\boldsymbol{t}$ and $\boldsymbol{y}$, such that $\boldsymbol{t}\to\boldsymbol{t}^{\boldsymbol{y}}$ is an automorphism of $A_{(L)}$ (for any perfect field L containing $K[[\boldsymbol{y}]]$), and $(\boldsymbol{t}^{\boldsymbol{y}})^{\boldsymbol{y}'} = \boldsymbol{t}^{\boldsymbol{y}'\boldsymbol{y}}$ for two independent points $\boldsymbol{y}$, $\boldsymbol{y}'$ of B; it is then easily verified that we define a group G by taking as group law

$$\phi((\boldsymbol{t},\boldsymbol{y}),(\boldsymbol{t}',\boldsymbol{y}')) = (\boldsymbol{t}\boldsymbol{t}'^{\boldsymbol{y}},\boldsymbol{y}\boldsymbol{y}').$$

We say that G is the *semi-direct product* of A and B, corresponding to the automorphism $\boldsymbol{t}\to\boldsymbol{t}^{\boldsymbol{y}}$; it is obvious that the homomorphisms $\boldsymbol{u}\colon\boldsymbol{t}\to(\boldsymbol{t},\boldsymbol{e})$ and $\boldsymbol{v}\colon(\boldsymbol{t},\boldsymbol{y})\to\boldsymbol{y}$ constitute with G an extension of B by A, and when A is abelian, it is clear that such an extension is trivial, and conversely, that the sums on both sides being taken for the group law of A. Observe first that replacing t by 0 in (18) gives $f(s,0) = f(0,u)$, and as s and u are distinct indeterminates, this implies $f(s,0) = f(0,u) = 0$. It also follows from (18) that $f_1(s,t) = f(s,t) + f(t,s)$ is also a 2-cocycle, and as $f_1(t,s) = f_1(s,t)$, it defines an *abelian* extension of I_∞ by A. However, we know that such an extension is quasi-trivial [10, p. 122, Prop. 4], hence (Prop. 2) there is an integer $r \geqq 0$ and a 1-cochain $\boldsymbol{c} \in C^1(I_\infty, A^{(r)})$ such that

$$(19) \qquad \boldsymbol{p}^r(f(s,t) + f(t,s)) = \boldsymbol{c}(s) - \boldsymbol{c}(s+t) + \boldsymbol{c}(t).$$

If $p \neq 2$, $\boldsymbol{x} \rightarrow 2 \cdot \boldsymbol{x}$ is an automorphism of $A^{(r)}$, hence there is a 1-cochain $\boldsymbol{c}_1 \in C^1(I_\infty, A^{(r)})$ such that $\boldsymbol{c}(s) = 2 \cdot \boldsymbol{c}_1(s)$; if we denote by $f_2(s,t)$ the 2-cocycle $\boldsymbol{p}^r(f(s,t)) - \boldsymbol{c}_1(s) + \boldsymbol{c}_1(s+t) - \boldsymbol{c}_1(t)$, (19) can be written $f_2(s,t) + f_2(t,s) = 0$. For $p = 2$, $\boldsymbol{x} \rightarrow 2 \cdot \boldsymbol{x}$ is only an isogeny, and therefore we can only assert the existence of an integer $h \geqq 0$ and a 1-cochain $\boldsymbol{c}_1$ such that $\boldsymbol{p}^h(\boldsymbol{c}(s)) = 2 \cdot \boldsymbol{c}_1(s)$; we will then take

$$f_2(s,t) = \boldsymbol{p}^{r+h}(f(s,t)) - \boldsymbol{c}_1(s) + \boldsymbol{c}_1(s,t) - \boldsymbol{c}_1(t),$$

and we reach the same conclusion. Using Prop. 2, we see that the proof of Prop. 5 is reduced to that of the following statement: *a 2-cocycle* $f \in Z^2(I_\infty, A)$ *such that*

$$(20) \qquad f(s,t) + f(t,s) = 0$$

is equal to 0.

We first remark that if in (18) we take $u = s$, then equation (20) yields $2 \cdot f(s+t,s) = 2 \cdot f(t,s)$, and as A is divisible, this gives

$$(21) \qquad f(s+t,s) = f(t,s),$$

hence also, by (20),

$$(22) \qquad f(s,s+t) = f(s,t).$$

If we replace t in succession by $0, s, 2s, \cdots$, in (21), we get

$$(23) \qquad f(ks,s) = 0 \text{ for every integer } k > 0.$$

We claim that for any integer $k > 0$

$$(24) \qquad f(ks,u) = k \cdot f(s,u).$$

Use induction on k: replace s by ks and t by s in (18); by (23), we get $f((k+1)s,u) = f(ks,s+u) + f(s,u)$; the inductive assumption and (22) yield $f(ks,s+u) = k \cdot f(s,s+u) = k \cdot f(s,u)$, hence our assertion. Let now $k = p$ in (24); we have $p \cdot f(s,u) = 0$ and as A is divisible, this means $f(s,u) = 0$, q. e. d.

COROLLARY. *Any solvable Lie group G (over an algebraically closed field) is isogeneous to a group G_1 which is the direct product of a divisible abelian group and of a semi-direct product of the largest unipotent subgroup of G_1 and of a torus.*

7. Two-dimensional Lie groups. We now know enough to give a complete description, up to isogeny, of all two-dimensional Lie groups over an algebraically closed field. If such a group G is abelian, its structure (up to isogeny) is described by Theorems 1 and 2 of [10], restricted to the case $n = 2$. On the other hand, it follows from Chevalley's theory [3] that G cannot be a simple non abelian group [9, p. 385, Th. 7] since such a group is at least 3-dimensional. If G is not an abelian group, it therefore contains a normal subgroup N of dimension 1; there are then two possible cases:

A) G is nilpotent; N is the center of G (the center of a nilpotent group cannot be reduced to $\boldsymbol{e}$);

B) G is solvable but not nilpotent; then the center of G is reduced to $\boldsymbol{e}$ (otherwise G would be nilpotent); hence, it follows from Theorem 2 that G is a semi-direct product of N and of a 1-dimensional torus T.

Case A. From Prop. 4 it follows that G/N cannot be a torus; on the other hand, G/N is a one-dimensional representable abelian group, hence can only be I_∞ [9, p. 379, Prop. 37]. From Prop. 5, it then follows that N cannot be divisible (otherwise G would be commutative), and therefore we also have $N = I_\infty$. The structure of G is then known if we can describe all central extensions of I_∞ by itself. This, however, has essentially been done by M. Lazard: he has determined all homogeneous polynomials $P(x,y)$ in two indeterminates, which satisfy the equation

$$P(x+y,z) + P(x,y) = P(x,y+z) + P(y,z)$$

[12, pp. 261-264], and any 2-cocycle f on I_∞ with values in I_∞ is clearly an infinite sum of such polynomials; of course, to get a noncommutative group G we have to take at least one of these polynomials such that $P(y,x) \neq P(x,y)$.

The nilpotent groups thus defined give rise to a number of interesting remarks. First, they obviously constitute a phenomenon which is special to characteristics $p > 0$, since it is well known that there are no nilpotent non abelian Lie algebras of dimension 2 over a field of characteristic 0. We next observe that N is the *unique* subgroup of G of dimension 1: any other such subgroup H would be commutative and commute with N, and moreover, we would have necessarily $H \wedge N = \boldsymbol{e}$, hence $G = H \vee N$ [9, p. 354, Prop. 11], and therefore G would be a quasi-direct product of H and N (see Section 5), hence would be commutative. It follows that G is not the l. u. b. of all abelian subgroups of G, which disproves a natural conjecture made in [7, p. 443].

We will next prove the rather surprising result:

PROPOSITION 6. *There exists a unipotent non commutative group G of dimension 2 which is not representable.*

This will prove, in particular, that a central extension of a representable group by a representable group (in this case, both are I_∞) is not necessarily representable; the class of non representable Lie groups is thus much more extensive than might have been thought *a priori*. It will also do away with any hope of extending to formal Lie groups either Ado's theorem or Chevalley's theorem on the structure of general algebraic groups [13, p. 439, Th. 16] in a reasonable way: the natural conjecture would have been that a Lie group would be the quasi-direct product of a divisible abelian group and of a representable group, but our example will show that this is not even the case for nilpotent groups.

To construct our example, we suppose that the field K has an infinite degree of transcendancy over the prime field $\boldsymbol{F}_p$, and we denote by (e_{hk}) (for all pairs (h, k) of numbers such that $h > k \geqq 0$) a system of *algebraically independent* elements of K (over $\boldsymbol{F}_p$). We define the extension G by means of the 2-cocycle

$$f(x, x') = \sum_{h>k} e_{hk} x^{p^h} x'^{p^k},$$

the group law of G being therefore given by

$$\left\{\begin{array}{l} x'' = \phi_1(x, x') = x + x' \\ y'' = \phi_2(x, y, x', y') = y + y' + \sum_{h>k} e_{hk} x^{p^h} x'^{p^k}. \end{array}\right. \tag{25}$$

The subgroup N is a typical subgroup defined by $x = 0$. We shall slightly simplify our general notations by writing (for $x_1 = x$, $x_2 = y$) D_h and X_h instead of D_{h1} and X_{h1}, $Y_h = D_h'$ instead of $X_{h2} = D_{h2}$. From (25) and the definition of X_h [4, p. 93], we deduce

$$X_h = D_h + \Big(\sum_{m>h} e_{mh} x^{p^m}\Big) D_0' + S_h, \tag{26}$$

where S_h is a combination (with coefficients in $\boldsymbol{F}_p$) of terms each of which is a product of a certain number of terms $e_{ij} x^{p^i}$ with $j < h$, and of a certain number of D'_j and D_j with $j < h$. For $h = 0$, $S_h = 0$, hence

$$[X_h, X_0] = e_{h0} Y_0. \tag{27}$$

If we want to compute similarly $[X_h, X_k]$ for $h > k$, we have (by definition) to form $D_h X_k - D_k X_h$ and to replace x by 0 in the result. We thus obtain

$$[X_h, X_k] = \bar{e}_{hk} Y_0 + \sum_{\alpha} \bar{e}_{hk\alpha} Z_\alpha, \tag{28}$$

where the Z_α have their usual meaning (elements of the structural basis, with of course $\alpha = (\alpha_1, \alpha_2)$), and the summation extends over the indices such that $|\alpha| \neq 1$ and $h(\alpha) < h$; in addition

$$\bar{e}_{hk} = e_{hk} - F_{hk}((e_{ij})), \tag{29}$$

where F_{hk} is a polynomial *with coefficients in $\boldsymbol{F}_p$*, in the e_{ij} such that either $i \leqq h$ and $j < k$, or $i < h$ (this is due to the fact that $D_k x^{p^i} = 0$ for $i > k$), and $\bar{e}_{hk,\alpha}$ is a polynomial, with coefficients in $\boldsymbol{F}_p$, in the e_{ij} such that either $i \leqq h$ and $j < k$, or $i < h$ (for the same reason). Similarly, if we express the X_c as linear combinations of the Z_λ, we see that if $h(\alpha) < h$, the coefficients are polynomials, with coefficients in $\boldsymbol{F}_p$, in the e_{ij} such that $i < h$. The group law of G will not in general be pseudo-canonical; but if we apply to it the "standard process" described in [9, p. 335] to transform it into a pseudo-canonical group law, it follows easily from our last remark and from the fact that in the free hyperalgebra the coefficients of the multiplication table are in $\boldsymbol{F}_p$, that after we have made the necessary change of variables, we still have (28) with similar properties for the coefficients $\bar{e}_{hk}$ and $\bar{e}_{hk\alpha}$ (although, of course, the polynomials F_{hk} will not be the same). We may therefore assume that the group law of G is pseudo-canonical.

We shall now assume that G is representable and show that this ultimately leads to a contradiction. Our assumption is therefore that there is a two-dimensional subgroup G' of a group $GL(n)$ (over K) which is isogeneous to G. Replacing, if necessary, G by some $G^{(r)}$, we can assume that there is an isogeny $\boldsymbol{u}$ of G onto G', and furthermore, that there is no trivial factor $\boldsymbol{p}$ in that isogeny. If we denote by $\mathfrak{G}$ (resp. $\mathfrak{G}'$, $\mathfrak{G}''$) the hyperalgebra of G (resp. G', $GL(n)$), by $\mathfrak{g}_h$ and $\mathfrak{s}_h$ (resp. $\mathfrak{g}_h'$, $\mathfrak{g}_h''$ and $\mathfrak{s}_h'$, $\mathfrak{s}_h''$) the Lie algebra of invariant semi-derivations of height h and the associative subalgebra it generates in $\mathfrak{G}$ (resp. $\mathfrak{G}'$, $\mathfrak{G}''$), our last assumption means that, for the derived mapping $\boldsymbol{u}' \colon \mathfrak{G} \to \mathfrak{G}'$, we have $\boldsymbol{u}'(\mathfrak{g}_0) \neq 0$. Let $\mathfrak{a}$ be the kernel of $\boldsymbol{u}'$, which is a two-sided ideal in $\mathfrak{G}$; if $\mathfrak{a} \neq 0$, we have $\mathfrak{a} \cap \mathfrak{g}_0 \neq 0$ (by the homomorphism theorem), and it follows from (27) that $\mathfrak{a} \cap \mathfrak{g}_0$ is the subspace consisting of the scalar multiples of Y_0. We next observe that, due to (27) and to the existence of the Frobenius homomorphism, the coefficient of Y_k on the right hand side of (28) is ${e^{p^k}}_{h-k,0} \neq 0$. It is then easy to see that $\mathfrak{a}$ is the ideal generated by $Y_0, Y_1, \cdots, Y_{t-1}$ in G, if $\boldsymbol{u}$ is an isogeny of height t; this can be done either directly by using an argument similar to the proof of Theorem 1 in [9, p. 339-340], or by applying general characterizations of kernels of derived mappings of isogenies, which will be described in detail in a forthcoming publication of P. Cartier (see preliminary announcement in [2]); for that reason, we suppress the proof here. We can then write $\boldsymbol{u} = \boldsymbol{w} \circ \boldsymbol{v}$, where $\boldsymbol{v}$ is an isogeny of G onto a group $\bar{G}$, $\boldsymbol{w}$ an isomorphism of $\bar{G}$ onto G', and where $\bar{G}$ is the extension of I_∞ by itself corresponding to the 2-cocycle f^{p^t}.

We shall from now on replace G by $\bar{G}$; ignoring the effect of the automorphism $\xi \rightarrow \xi^{p^t}$ on the e_{hk}, we are thus reduced to proving that after replacing the e_{hj} for $j < t$ by 0 in our description of G, there can be no *isomorphism* $\boldsymbol{u}$ of G onto a subgroup G' of $GL(n)$. It is clear that if we write $X_h' = \boldsymbol{u}'(X_k)$, $Y_h' = \boldsymbol{u}'(Y_h)$, $Z_\alpha' = \boldsymbol{u}'(Z_\alpha)$, the Z_α' constitute a structural basis of $\mathfrak{G}'$, for which the group law of G' is pseudo-canonical: in other words, Z_α' is equal to a noncommutative polynomial in the X_k' and Y_k' such that $k \leqq h(\alpha)$, *with coefficients in* $\boldsymbol{F}_p$. Using this fact, we will now prove the following statement:

(*) *There is an increasing sequence* (L_h) *of fields over* $\boldsymbol{F}_p$, *such that* L_h *is generated over* $\boldsymbol{F}_p$ *by* $2n^2(h+1)$ *elements, and that the* Z_α' *with* $h(\alpha) \leqq h$ *are linear combinations of the basis of* $\mathfrak{g}_h''$ *with coefficients in* L_h.

We use induction on h: for $h = 0$, X_0' and Y_0' are linear combinations of the basis of $\mathfrak{g}_0''$; we take for L_0 the field generated over $\boldsymbol{F}_p$ by the $2n^2$ coefficients of these linear combinations. We assume throughout that we have taken the group law in $GL(n)$ in its natural form [9, p. 364] so that the multiplication table of the corresponding basis of $\mathfrak{G}''$ has its coefficients in $\boldsymbol{F}_p$. We denote by Δ the "structural mapping" of $\mathfrak{G}''$ into $\mathfrak{G}'' \otimes \mathfrak{G}''$, which induces the structural mapping of $\mathfrak{G}'$ into $\mathfrak{G}' \otimes \mathfrak{G}'$. The element X_h' satisfies the relation

$$\Delta(X_h') - 1 \otimes X_h' - X_h' \otimes 1 = \sum Z_\alpha' \otimes Z_\beta' \tag{30}$$

the summation being extended to all pairs such that $|\alpha| \neq 1$, $|\beta| \neq 1$, $\alpha + \beta = p^h \epsilon_1$. If we express X_h' as a linear combination of the basis of $\mathfrak{g}_h''$, relation (30) is equivalent to a system of (non homogeneous) linear equations, where the unknowns are the coefficients of that linear combination, and the coefficients and right hand terms are *in the field* L_{h-1}, due to our inductive assumption. We know that there is an element X_h' in $\mathfrak{G}'$ which satisfies (30); this means that the equivalent system of linear equations has a solution consisting of *elements of* K; but from the preceding remark, it follows that it has also a solution consisting of *elements of* L_{h-1}. Let X_h'' be the element of $\mathfrak{G}''$ which is determined by that second solution; we shall have in general $X_h'' \neq X_h'$, but it follows from (30) that the difference $X_h'' - X_h'$ is a *derivation*, in other words, it belongs to $\mathfrak{g}_0''$. Similarly, there is an element Y_h'' in $\mathfrak{G}''$ which is a linear combination of the basis of $\mathfrak{g}_h''$ with coefficients in L_{h-1}, and such that $Y_h'' - Y_h'$ is in $\mathfrak{g}_0''$; if we express these two elements of $\mathfrak{g}_0''$ as linear combinations of the basis of that Lie algebra, and denote by L_h the field obtained by adjoining to L_{h-1} the coefficients of these combinations ($2n^2$ in all), we have shown that the basis of $\mathfrak{g}_h'$ can be expressed as linear combinations of the basis of $\mathfrak{g}_h''$ with coefficients in L_h. It follows that the coefficients of the multiplication table for the basis of $\mathfrak{g}_h'$ belong to L_h. The other elements Z_α' of the basis of $\mathfrak{z}_h'$ are therefore (by the remark preceding statement (*)) linear combinations of the basis of $\mathfrak{z}_h''$ with coefficients in L_h, and our induction is thus complete.

We are now ready to derive our final contradiction. For any h, it follows from (*) and (28) that the coefficients $\bar{e}_{ij}$ $(j < i \leqq h)$ belong to L_h. However, there are $(h-t)(h-t+1)/2$ such elements which are algebraically independent over $\boldsymbol{F}_p$; hence the inequality

$$(h-t)(h-t+1)/2 \leqq 2n^2(h+1)$$

which certainly cannot be verified when h is taken large enough; q. e. d.

If we do not assume that the e_{hk} are algebraically independent, we can, of course, obtain representable groups, and even algebraic groups: the simplest of these is the group of 3×3 matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & x^p & 1 \end{pmatrix}.$$

More generally, if in the preceding matrix, we replace x^p by

$$g(x) = e_1 x^p + e_2 x^{p^2} + \cdots + e_h x^{p^h} + \cdots,$$

where the e_h are arbitrary elements of K, we define a monomorphism into $GL(3)$ of the group G corresponding to the 2-cocycle

$$f(x, x') = \sum_{h \geqq 1} e_h x^{p^h} x'. \tag{31}$$

We can, however, prove

PROPOSITION 7. *If in* (31) *the* e_h *are algebraically independent over* $\boldsymbol{F}_p$, *then* G *is not an algebraic group* (or, more precisely, G cannot be *isogeneous* to a formal Lie group of the type G'^*, where G' is an algebraic group).

In other words, if we consider in *any* $GL(n)$ a formal subgroup G_1 isogeneous to G, we shall always have $\dim \mathfrak{A}(G_1) > \dim G_1$ for its algebraic hull $\mathfrak{A}(G_1)$.

We may suppose that K is algebraically closed without restricting the generality. We first investigate the structure of an algebraic group G' which has a center C' isomorphic to the additive group K, and which is such that G'/C' is also isomorphic to K: indeed, if G is isogenous to G'^*, G' will necessarily be of this type, for the center C of G has then to be isogeneous to C'^*, and G/C to G'^*/C'^* [9, Props. 18 and 21], and there is only one algebraic group formally isogeneous to I_∞, namely the additive group K. Now, a result of Rosenlicht [13, p. 426, Th. 10] proves the existence of a (rational) cross-section $\sigma\colon G'/C' \rightarrow G'$; this cross-section will in general only be defined in an open set U of K (for the Zariski topology), but we shall show that there is then another cross section which is *everywhere defined* in K. Indeed, let u be a biregular isomorphism of the additive group K onto the center C' (which, like G', we write multiplicatively). If π is the natural homomorphism of G' onto G'/C' (which we identify with K), let $\rho(s) = s\cdot(\sigma(\pi(s)))^{-1}$; this is a rational mapping of G' into C', defined in $\pi^{-1}(U)$. The complement of U in K consists of a *finite* number of points x_i $(1 \leqq i \leqq m)$; let $x_0 \in U$ be such that all the points $x_0 + x_i$ $(1 \leqq i \leqq m)$ are also in U, and consider the rational function (from K to K)

$$\phi(x) = u^{-1}(\rho(\sigma(x)\sigma(x_0)));$$

at each of the points x_i $(1 \leqq i \leqq m)$ this function may have a pole; there is, at any rate, a rational function $\psi(x)$ which has poles *at most* at the x_i $(1 \leqq i \leqq m)$, and is such that $\phi(x) - \psi(x)$ is *regular* at all these points. Consider then the cross-section

$$\sigma'(x) = \sigma(x)(u(\psi(x)))^{-1};$$

it is certainly regular outside the x_i $(1 \leqq i \leqq m)$; we show that it is also regular at these points. Indeed, we have

$$\sigma'(x)\sigma(x_0) = \sigma(x)\sigma(x_0)(u(\psi(x)))^{-1} = \psi(x+x_0)u(\phi(x) - \psi(x)),$$

and as the right hand side is regular at each of the x_i, so is $\sigma'(x)$.

We may thus suppose that σ is regular on K; then ρ is also defined everywhere on G, and

$$a(x,x') = u^{-1}(\rho(\sigma(x)\sigma(x')))$$

is a 2-cocycle which is a rational function *defined everywhere* on $K \times K$, hence a *polynomial* in x and x'. We conclude that there is a biregular isomorphism of G' onto a group G_1 defined by the group law

$$(32) \qquad \begin{cases} \phi_1^{(1)}(x, x') = x + x' \\ \phi_2^{(1)}(x, y, x', y') = y + y' + f_1(x, x'), \end{cases}$$

where f_1 is a polynomial 2-cocycle.

We now proceed to show that there is no isogeny of G_1 onto G. By the same argument as in the proof of Prop. 6, one is immediately reduced to proving that there is no *isomorphism* $\boldsymbol{u} = (u_1(x, y), u_2(x, y))$ of G_1 onto G. Such an isomorphism must of course map the center C_1 of G_1 onto the center C of G; hence, the relation $x = 0$ must imply $u_1(0, y) = 0$; this means that in the power series $u_1(x, y)$, every monomial contains x. However, we must have

$$(33) \qquad u_1(x + x', y + y' + f_1(x, x')) = u_1(x, y) + u_1(x', y'),$$

and if $u_1(x, y)$ actually contained y, by considering the monomials of smallest degree in y, and among them, the one with smallest degree in x (the latter being $\neq 0$, as seen above), it is clear that there would be in the left hand side of (33) terms containing both x' and y, which cannot be matched by similar terms on the right hand side. Hence u_1 must be an additive power series in x, i. e.

$$u_1(x) = a_0 x + a_1 x^p + \cdots + a_k x^{p^k} + \cdots \qquad (a_0 \neq 0).$$

A similar argument, applied to the relation

$$(34) \quad u_2(x + x', y + y' + f_1(x, x')) = u_2(x, y) + u_2(x', y') + f(u_1(x), u_1(x'))$$

shows that there are no monomials in $u_2(x, y)$ which can contain both x and y, i. e. $u_2(x, y) = v(x) + w(y)$. Replacing x and x' by 0 in (34) shows that w is an additive power series, i. e.

$$w(y) = b_0 y + b_1 y^p + \cdots + b_k y^{p^k} + \cdots \qquad (b_0 \neq 0),$$

and then (34) boils down to

$$(35) \qquad g(u_1(x)) \cdot u_1(x') = v(x + x') - v(x) - v(x') + w(f_1(x, x')).$$

We claim that it is impossible that *both* $g \circ u_1$ and u_1 be polynomials: indeed, this would imply that the relations

$$e_k b_0^{p^k} + e_{k-1} b_1^{p^{k-1}} + \cdots + e_1 b_{k-1} = 0$$

hold from a certain k on, with only finitely many of the b_k being $\neq 0$; but this would obviously imply that the e_k are not algebraically independent over $\boldsymbol{F}_p$. However, if $g \circ u_1$ has infinitely many terms, there are on the left hand side of (35) terms of the form $x^{p^k} x'$ with arbitrarily high values of k.

But in $w(f_1(x,x'))$, the terms of the form $x^h x'$ have *bounded* exponents h since f_1 is a polynomial, and if there were in $v(x+x')-v(x)-v(x')$ a term in $x^{p^k}x'$, there would be a term in xx'^{p^k} (with same coefficient) which cannot be cancelled by terms of $w(f_1(x,x'))$ for the same reason as above, and is not matched by any term on the left hand side. If on the contrary, $g\circ u_1$ is a polynomial, then u_1 has infinitely many terms $\neq 0$; hence there are on the left hand side terms in $x^p x'^{p^k}$ with arbitrarily high k, and no terms in $x^{p^k}x'^p$ as soon as k is large enough; an argument quite similar to the preceding one shows that (35) is again impossible in that case, and the proof of Prop. 7 is complete.

8. *Case B.* In sharp contrast with the rather pathological features of case A, we shall prove

PROPOSITION 8. *Every solvable non nilpotent group G of dimension 2 is isomorphic to one of the (algebraic) groups of matrices*

$$\begin{pmatrix} 1+s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & (1+s)^{p^h} \end{pmatrix}$$

and all these groups are isogeneous.

As G is a semi-direct product of a normal subgroup isomorphic to I_∞ and of a subgroup isomorphic to I_0, we have to determine all the possible structures of I_0-module on I_∞. As $x\rightarrow s\cdot x$ is an automorphism of I_∞ (over a field containing $K[[s]]$), we can write $s\cdot x=\sum_{k=0}^{\infty} a_k(s)x^{p^k}$. It is readily verified that the group of automorphisms of I_∞ can be considered as an infinite dimensional formal Lie group A, which is recursive in the sense of [6, p. 55], and can be neatly described, in a self-explanatory way, as the group of infinite triangular matrices

$$\begin{pmatrix} 1+x_1 & x_2 & x_3 & \cdots & x_n & \cdots \\ 0 & (1+x_1)^p & x_2^p & \cdots & x_{n-1}^p & \cdots \\ 0 & 0 & (1+x_1)^{p^2} & \cdots & x_{n-2}^{p^2} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & (1+x_1)^{p^{n-1}} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}. \tag{36}$$

The system of power series $(a_k(s))$ constitutes a homomorphism $s\rightarrow M(s)$ of I_0 into that group A; equivalently, this means that for every n, the first

n series $a_k(s)$ constitute a homomorphism $s \to M_n(s)$ of I_0 into the group A_n obtained by taking only the first n rows and columns in the infinite matrix (36). In particular, $A_1 = I_0$, and therefore we must have $1 + a_0(s) = (1+s)^\zeta$, where ζ is an arbitrary p-adic integer [5, p. 241, Th. 5]. We claim now that for any k, $a_k(s)$ is a linear combination of the power series $(1+s)^{p^h\zeta} - (1+s)^\zeta$ for $0 \leqq h \leqq k$. To prove this, we use induction on k and observe that the group A_n, which has dimension n, is a semi-direct product of a nilpotent group and of a one-dimensional torus, namely the subgroup of diagonal matrices $(1+x_1, (1+x_1)^p, \cdots, (1+x_1)^{p^{n-1}})$. We may assume $\zeta \neq 0$, otherwise it would be easily checked that all the a_k of index $k \geqq 1$ would be 0 (there is no homomorphism $\neq 0$ of I_0 into a unipotent group); from A. Borel's conjugation theorem [1, p. 56, Th. 12.2] it follows that there is a unipotent triangular matrix P_k of order k such that $P_k M_k(s) P_k^{-1}$ is the diagonal matrix $((1+s)^\zeta, \cdots, (1+s)^{p^{k-1}\zeta})$. If we denote by P the infinite triangular matrix $\begin{pmatrix} P_k & 0 \\ 0 & I \end{pmatrix}$, we see that by replacing the homomorphism $s \to M(s)$ by $s \to PM(s)P^{-1}$, we may suppose that $a_1(s) = \cdots = a_{k-1}(s) = 0$. The relation $M(s+t+st) = M(s)M(t)$ then yields, in particular,

$$\begin{aligned} a_k(s+t+st) &= (1+s)^\zeta a_k(t) + a_k(s)\,(1+t)^{p^k\zeta} \\ &= (1+t)^\zeta a_k(s) + a_k(t)\,(1+s)^{p^k\zeta}, \end{aligned}$$

and as t and s are independent indeterminates, this is only possible if $a_k(s) = c_k((1+s)^{p^k\zeta} - (1+s)^\zeta)$. Returning to our original $M(s)$, this proves our assertion.

Now let $\zeta = p^h\epsilon$, where ϵ is a p-adic unit. In the group G, we may change variables by taking new variables s_1, x_1 such that $1 + s_1 = (1+s)^\epsilon$ and $x_1 = x$. The new group law corresponds to a structure of I_0-module on I_∞ in which $\zeta = p^h$; we may thus assume from now on that this condition is satisfied. It is then clear that we have

$$s \cdot x = (1+s)^q c_0(x) + (1+s)^{pq} c_1(x^p) + \cdots + (1+s)^{p^n q} c_n(x^{p^n}) + \cdots,$$

where $c_0(x) = x + c_{01}x^p + \cdots$ and, in general,

$$c_n(x) = c_{n0}x + c_{n1}x^p + \cdots + c_{nm}x^{p^m} + \cdots,$$

and we have written for simplicity $q = p^h$. We then change variables again, taking this time $s_1 = s$ and $x_1 = c_0(x)$; this amounts (again dropping the indices 1) to supposing that $c_0(x) = x$; but if we then again write relation (5), we see easily that the $c_n(x)$ of index $\geqq 1$ must be 0: supposing in fact that r is the first index such that $c_r(x) \neq 0$, we see that in the identity, the term $(1+s)^q(1+t)^{qp^r}c_r(x^{p^r})$ is not matched by any other term, hence the assumption $c_r \neq 0$ leads to a contradiction. This ends the proof of Prop. 8, and we thus see that for characteristic $p \neq 0$, the structure of solvable non nilpotent groups of dimension 2 is pretty much the same as for characteristic 0, if we disregard the isogenies. I do not know if this extends to dimensions $\geqq 3$.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956), pp. 20-82.

[2] P. Cartier, "Calcul différentiel sur les variétés algébriques en caractéristique non nulle," *Comptes Rendus Hebdomadaires des Séances de l'Academie des Sciences, Paris*, vol 245 (1957), pp. 1109-1111.

[3] C. Chevalley, "Classification des groupes de Lie algébriques," *Séminaire École Normale Supérieure*, 1956-57.

[4] J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$," *Commentarii Mathematici Helvetici*, vol. 28 (1954), pp. 87-118.

[5] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, (II)," *American Journal of Mathematics*, vol. 77 (1955), pp. 218-244.

[6] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, (III)," *Mathematische Zeitschrift*, vol. 63 (1955), pp. 53-75.

[7] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV)," *American Journal of Mathematics*, vol. 77 (1955), pp. 429-452.

[8] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (V)," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 207-239.

[9] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI)," *American Journal of Mathematics*, vol. 79 (1957), pp. 331-388.

[10] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (VII)," *Mathematische Annalen*, vol. 134 (1957), pp. 114-133.

[11] G. Hochschild-J-P. Serre, "Cohomology of group extensions," *Transactions of the American Mathematical Society*, vol. 74 (1953), pp. 110-134.

[12] M. Lazard, "Sur les groupes de Lie formels à un paramètre," *Bulletin de la Société Mathématique de France*, vol. 83 (1955), pp. 251-274.

[13] M. Rosenlicht, "Some basic theorems on algebraic groups," *American Journal of Mathematics*, vol. 78 (1956), pp. 401-443.

ON SOME INVARIANTS OF CYCLOTOMIC FIELDS.*

By KENKICHI IWASAWA.**

Dedicated to Professor E. Artin on His Sixtieth Birthday

1. Let p be an odd prime. For each $n \geqq 0$, we denote by ζ_n a primitive p^n-th root of unity and by K_n the cyclotomic field obtained by adjoining ζ_{n+1} to the rational field Q: $K_n = Q(\zeta_{n+1})$. It is proved in [4] that if p^{e_n} is the highest power of p dividing the class number of K_n, then the exponent e_n is given, for all sufficiently large n, by a formula

$$e_n = \lambda n + \mu p^n + \nu, \qquad n \geqq n_0, \tag{1}$$

where λ, μ and ν are integers independent of n. The numbers λ and μ seem to have deep significance for the arithmetic of the fields K_n. In general, if the invariant $\mu = \mu(K/F)$ of a so-called Γ-extension K over a finite algebraic number field F is 0, then the Galois group of the maximal unramified abelian p-extension over K is, up to a finite subgroup, isomorphic with the direct sum of λ copies of the additive group of p-adic integers, where $\lambda = \lambda(K/F)$ denotes another invariant of K/F.[1] So, if $\mu = 0$, we have an analogue, for number fields, of a similar result for algebraic function fields of one variable over algebraically closed fields of constants. For this and other reasons, it seems interesting to know whether $\mu > 0$ or $\mu = 0$ for a given Γ-extension K/F, and we shall find in the present paper necessary and sufficient conditions for $\mu > 0$ when the Γ-extension is obtained from the cyclotomic fields K_n defined above, namely, when μ is given as the second coefficient in the above formula (1).

2. Let K be the union of all K_n, $n \geqq 0$. K is an abelian extension of Q and, for any element σ of the Galois group $G(K/Q)$, there exists a unique p-adic unit ξ such that

$$\sigma(\zeta_n) = \zeta_n^{\xi},$$

for every $n \geqq 0$. The mapping $\sigma \rightarrow \xi$ then defines a topological isomorphism

---

* Received February 6, 1958.

** Guggenheim Fellow. The present research was also supported in part by a National Science Foundation grant.

[1] Cf. [4], § 5, § 7.

of $G(K/Q)$ with the multiplicative group U of p-adic units and we denote the Galois automorphism σ corresponding to ξ by σ_ξ. Under this isomorphism, the subgroup $G(K/K_n)$ of $G(K/Q)$ corresponds to the subgroup U_n of all ξ in U satisfying $\xi \equiv 1 \bmod. p^{n+1}$. On the other hand, the group U is the direct product of U_0 and a cyclic group V of order $p-1$, the group of all roots of unity in the p-adic number field Q_p. The corresuonding subgroup Δ of $G(K/Q)$ is then canonically isomorphic with the Galois group $G(K_0/Q)$, and $G(K/Q)$ is the direct product of Δ and $\Gamma = G(K/K_0) \cong U_0$.

Now, suppose that Δ acts continuously on a compact p-primary abelian group N. Since N is p-primary, the element u^α is defined as usual for any u in N and for any p-adic integer α. For each i, $1 \leqq i \leqq p-1$, let $N^{(i)}$ be the set of all u in N such that

$$\sigma_\eta(u) = u^{\eta^i},$$

for every η in V, i.e., for every σ_η in Δ. It is then easy to see that each $N^{(i)}$ is a closed subgroup of N and N is the direct product of these $N^{(i)}$:

$$N = N^{(1)} \times \cdots \times N^{(p-1)}.$$

Let L be the maximal unramified abelian p-extension over K. Then L is a Galois extension of Q, and $G(K/Q) = \Gamma \times \Delta$ acts on the abelian normal subgroup $G(L/K)$ of $G(L/Q)$ in a natural way. For each $n \geqq 0$, let L_n denote the maximal unramified abelian p-extension of K_n. L is then the union of all L_n and, p^{e_n} being the degree of the extension L_n/K_n, the formula (1) was proved in [4] by studying the structure of the Γ-group $G(L/K)$.

We now apply the above decomposition to the Δ-group $G(L/K)$ and obtain

$$G(L/K) = G(L/K)^{(1)} \times \cdots \times G(L/K)^{(p-1)}.$$

We denote by $L^{(i)}$ $(1 \leqq i \leqq p-1)$ the subfield of L containing K such that

$$G(L/L^{(i)}) = \prod_{j \neq i} G(L/K)^{(j)}, \qquad G(L^{(i)}/K) \cong G(L/K)^{(i)}.$$

Since Δ may be considered as acting on the Galois group $G(L_n/K_n)$ in a natural way, $G(L_n/K_n)$ can be also decomposed with respect to Δ and we obtain subfields $L_n^{(i)}$ $(1 \leqq i \leqq p-1)$ of L_n containing K_n, defined similarly as the above $L^{(i)}$. Clearly, the action of Γ on $G(L/K)$ commutes with the action of Δ on $G(L/K)$. Hence $G(L^{(i)}/K)$ $(1 \leqq i \leqq p-1)$ are again Γ-groups like $G(L/K)$. Using the fact that $L^{(i)}$ is the union of all $L_n^{(i)}$, $n \geqq 0$, it can be proved in the same way as in [4] that if $p^{e_n^{(i)}}$ is the degree of the extension $L_n^{(i)}/K_n$, then the exponent $e_n^{(i)}$ is given, for all sufficiently large n, by

$$e_n^{(i)} = \lambda^{(i)} n + \mu^{(i)} p^n + \nu^{(i)}, \qquad (1 \leqq i \leqq p-1), \tag{2}$$

where $\lambda^{(i)}$, $\mu^{(i)}$ and $\nu^{(i)}$ are again integers independent of n. Since $e_n = \sum_{i=1}^{p-1} e_n^{(i)}$, we obtain from (1) and (2) that

$$\lambda = \sum_{i=1}^{p-1} \lambda^{(i)}, \qquad \mu = \sum_{i=1}^{p-1} \mu^{(i)}, \qquad \nu = \sum_{i=1}^{p-1} \nu^{(i)}.$$

Let e_n^+ be the sum of $e_n^{(i)}$ with even i and let e_n^- be the sum of $e_n^{(i)}$ with odd i. Similarly, we define λ^+, λ^-, μ^+, μ^- and ν^+, ν^- as the sums of $\lambda^{(i)}$, $\mu^{(i)}$ and $\nu^{(i)}$ with even or odd indices respectively. Then,

$$e_n = e_n^+ + e_n^-, \quad \lambda = \lambda^+ + \lambda^-, \quad \mu = \mu^+ + \mu^-, \quad \nu = \nu^+ + \nu^-.$$

Furthermore, if L_n^+ denotes the composite of all $L_n^{(i)}$ with even i and L_n^- the composite of all $L_n^{(i)}$ with odd i, then $p^{e_n^+}$ and $p^{e_n^-}$ are the degrees of the extensions of L_n^+/K_n and L_n^-/K_n respectively, and they are also equal to the highest powers of p dividing, respectively, the second and the first factors of the class number of K_n.[2]

LEMMA 1. *$\mu = 0$ if and only if $\mu^- = 0$.*

Proof. As the proof of (1) shows, $\mu = 0$ ($\mu^- = 0$) if and only if the rank of $G(L_n/K_n)$ ($G(L_n^-/K_n)$) is bounded for every $n \geqq 0$. However, it is a classical result that

$$\operatorname{rank} G(L_n^+/K_n) \leqq \operatorname{rank} G(L_n^-/K_n) \leqq \operatorname{rank} G(L_n/K_n) \leqq 2 \operatorname{rank} G(L_n^-/K_n).$$[3]

The lemma then follows immediately.

Remark. By a similar method as in [7], we can obtain a more precise result:

$$\operatorname{rank} G(L_n^{(i)}/K_n) \leqq \operatorname{rank} G(L_n^{(j)}/K_n), \qquad n \geqq 0,$$

where i is even, j is odd and $i + j \equiv 1 \bmod . p - 1$.

3. Assume, now, that $\mu > 0$. Then, by the above lemma, $\mu^- > 0$ and, hence, $\mu^{(i)} > 0$ for some odd index i. We fix such an index $i = a$. The Galois group $G(L^{(a)}/K)$ is then a so-called regular strictly Γ-finite compact Γ-group with the invariant $\mu^{(a)} > 0$, and it follows that, for each $n \geqq 0$, $G(L_n^{(a)}/K_n)$ contains a subgroup which is, as a $G(K_n/K_0)$-group, isomorphic with the additive group of the group ring of $G(K_n/K_0)$ over the prime field of characteristic p.[4] Let P_n be the p-Sylow group of the absolute ideal class group of K_n and let $P_n^{(a)}$ be the a-th direct factor of the Δ-decomposition of P_n. By class field theory, $G(L_n^{(a)}/K_n)$ is then canonically isomorphic with $P_n^{(a)}$. Hence, by the above, there exists an ideal class C_0 of order p in $P_n^{(a)}$ such that $\sigma_\eta(C_0)=C_0^{\eta^a}$ for every η in V and that the classes $\sigma_\xi(C_0)$ are independent when ξ runs over p-adic units in $U_0 \bmod. U_n$.

---

[2] More generally, if F is a subfield of K_0 with $[K_0 \colon F] = d$ and K' is the Γ-extension defined naturally over F, then the invariants of K'/F are given by the sums of $\lambda^{(i)}$ and $\mu^{(i)}$ with the indices i divisible by d.

[3] Cf. [7].

[4] Cf. [4], § 5 and a forthcoming paper of the author.

Now, for any p-adic integer α, let $s_n(\alpha)$ $(n\geqq 0)$ denote the uniquely determined rational integer such that

$$\alpha\equiv s_n(\alpha) \bmod. p^{n+1}, \qquad 0\leqq s_n(\alpha)<p^{n+1}.$$

For any ideal class C in P_n and for any ξ in U, we have then

$$\prod_\alpha \sigma_\alpha(C)^{d(\alpha)}=1, \tag{3}$$

where the product is taken over all α in $U \bmod. U_n$ and the exponent $d(\alpha)$ is given by

$$d(\alpha)=p^{-(n+1)}(s_n(\xi\alpha^{-1})-\xi s_n(\alpha^{-1})).$$

This is a special case of a general identity which holds for the ideal classes and their conjugates of a cyclotomic field. For the field K_0, it is given in [3], § 109 and the general case can be deduced easily from the result in [5].

Applying (3) to the above ideal class C_0, we obtain

$$\sum_{\eta\in V}(s_n(\xi\eta^{-1})-\xi s_n(\eta^{-1}))\eta^a\equiv 0 \bmod. p^{n+2}, \qquad \xi\in U,$$

or

$$\sum_\eta s_n(\xi\eta^{-1})\eta^a\equiv\xi\sum_\eta s_n(\eta^{-1})\eta^a \bmod. p^{n+2}, \qquad \xi\in U. \tag{4}$$

First, we put $\xi=1+p^{n+1}$ in the above. Since $s_n(\xi\eta^{-1})=s_n(\eta^{-1})$, we have

$$\sum_\eta s_n(\eta^{-1})\eta^a\equiv(1+p^{n+1})\sum_\eta s_n(\eta^{-1})\eta^a \bmod. p^{n+2},$$

and, hence, also

$$\sum_\eta s_n(\eta^{-1})\eta^a\equiv 0 \bmod. p.$$

As $s_n(\eta^{-1})\equiv\eta^{-1} \bmod. p$, it follows that $a\neq 1$.

Next, we take ξ from V, in (4). Then the left hand side is equal to $\xi^a\sum_\eta s_n(\eta^{-1})\eta^a$ and, as $a\neq 1$, $1\leqq a\leqq p-1$, it follows that

$$\sum_\eta s_n(\eta^{-1})\eta^a\equiv 0 \bmod. p^{n+2}.$$

Hence, by (4),

$$\sum_\eta s_n(\xi\eta^{-1})\eta^a\equiv 0 \bmod. p^{n+2}, \qquad \eta\in V, \tag{5}$$

for any ξ in U. We have thus proved that the assumption $\mu>0$ implies (5) for some odd index $a \neq 1$ and for every $n \geqq 0$. Notice that (5) does not hold for $a = 1$ (and $n = 0$).

To prove the converse of the above, we use the classical formula for the first factor of the class number of K_n.[5] Let Ω_p be the algebraic closure of Q_p and χ a character of U with values in Ω_p^* such that $\chi(U_n) = 1$. Put

$$S_n(\chi) = p^{-(n+1)} \sum_{\xi} s_n(\xi)\chi(\xi),$$

where ξ runs over p-adic units in $U \bmod. U_n$. We notice that $S_n(\chi)$ is an element of Ω_p and that if $\chi(U_m) = 1$ for $m \leqq n$, then $S_n(\chi) = S_m(\chi)$. Now, the classical formula tells us that the highest power of p dividing the first factor of the class number of K_n is equal to the highest power of p dividing, in Ω_p, the product

$$p^{n+1} \prod_{\chi} S_n(\chi), \tag{6}$$

where χ runs over all characters of U such that $\chi(U_n) = 1$ and $\chi(-1) = -1$.

Suppose that (5) holds for an odd index a. Clearly, there exist p^n characters χ of U such that $\chi(U_n) = 1$ and that $\chi(\eta) = \eta^{-a}$ for every η in V. Since a is odd, these characters satisfy $\chi(-1) = -1$ and the corresponding $S_n(\chi)$ appear in the product (6). It is also clear that (5) implies

$$S_n(\chi) \equiv 0 \bmod. p,$$

for any such character χ. On the other hand, it is known that the product of p^{n+1} and other factors $S_n(\chi')$ in (6) is an integer of Ω_p. Hence the product (6) is divisible by p^{p^n} and we obtain that

$$e_n^- \geqq p^n.$$

Since $e_n^- = \lambda^- n + \mu^- p^n + \nu^-$, it follows that if (5) holds for every $n \geqq 0$, then $\mu^- > 0$ and, consequently, $\mu > 0$. Thus the following result is proved:

I. *The second coefficient μ in the formula* (1) *is positive if and only if there exists an odd integer a, $1 \leqq a \leqq p-1$, such that* (5) *holds for any p-adic unit ξ and for any $n \geqq 0$.*

For any p-adic integer α, let

$$\alpha = \sum_{k=0}^{\infty} t_k(\alpha) p^k, \qquad 0 \leqq t_k(\alpha) < p,$$

be the canonical p-adic expansion of α. Then,

$$s_n(\alpha) = \sum_{k=0}^{n} t_k(\alpha) p^k, \qquad s_{n+1}(\alpha) = s_n(\alpha) + t_{n+1}(\alpha) p^{n+1}.$$

---

[5] For the following, cf. [2], § 5, § 33.

Since $a \neq 1$ and

$$\sum_{\eta} s_{n+1}(\xi\eta^{-1})\eta^{a} \equiv \sum_{\eta} \xi\eta^{a-1} \equiv 0 \bmod. p^{n+2},$$

the condition (5) is equivalent with the following:

$$\sum_{\eta} t_{n+1}(\xi\eta^{-1})\eta^{a} \equiv 0 \bmod. p, \qquad n \geqq 0.$$

Notice that it holds trivially

$$\sum_{\eta} t_{0}(\xi\eta^{-1})\eta^{a} \equiv 0 \bmod. p.$$

4. We now consider that the roots of unity ζ_n are all contained in Ω_p and asume that $\zeta_{n+1} = \zeta_n$, $n \geqq 0$. We have then

$$p^{n+1}/(\zeta_{n+1} - 1) = \sum_{i=0}^{p^{n+1}-1} i\zeta_{n+1}{}^{i} = \sum_{\alpha} s_n(\alpha)\zeta_{n+1}{}^{\alpha},$$

where α runs over all p-adic integers mod. p^{n+1}. For any η in V, it follows that

$$p^{n+1}/(\zeta_{n+1}{}^{\eta} - 1) = \sum_{\alpha} s_n(\alpha)\zeta_{n+1}{}^{\alpha\eta} = \sum_{\alpha} s_n(\alpha\eta^{-1})\zeta_{n+1}{}^{\alpha}.$$

If $n \geqq 1$, we have similarly

$$p^{n+1}/(\zeta_{n}{}^{\eta} - 1) = p\sum_{\beta} s_{n-1}(\beta\eta^{-1})\zeta_{n}{}^{\beta} = \sum_{\beta} s_n(p\beta\eta^{-1})\zeta_{n+1}{}^{p\beta},$$

where β runs over all p-adic integers mod. p^{n}. Therefore,

$$p^{n+1}(1/(\zeta_{n+1}{}^{\eta} - 1) - 1/(\zeta_{n}{}^{\eta} - 1)) = \sum_{\xi} s_n(\xi\eta^{-1})\zeta_{n+1}{}^{\xi},$$

where ξ runs over all p-adic units in U mod. U_n.

Now, for each $n \geqq 0$ and i, $1 \leqq i \leqq p-1$, put

$$T_n{}^{(i)} = \sum_{\eta \in V} \eta^{i}/(\zeta_{n+1}{}^{\eta} - 1).$$

Then the above computation shows that, for any $n \geqq 0$,

$$(7) \qquad p^{n+1}(T_n{}^{(i)} - T_{n-1}{}^{(i)}) = \sum_{\xi}\Big(\sum_{\eta} s_n(\xi\eta^{-1})\eta^{i}\Big)\zeta_{n+1}{}^{\xi}, \qquad \xi \text{ in } U \bmod. U_n.$$

For convenience, we put here

$$T_{-1}{}^{(i)} = 0, \qquad 1 \leqq i \leqq p-1.$$

Suppose that there exists an odd index a, $1 \leqq a \leqq p-1$, such that (5) holds for any p-adic unit ξ and for any $n \geqq 0$. Then, it follows from (7) that

$$T_n{}^{(a)} \equiv T_{n-1}{}^{(a)} \bmod. p, \qquad n \geqq 0,$$

and, as $T_{-1}^{(a)} = 0$, we also have that

$$T_n^{(a)} \equiv 0 \bmod. p, \qquad n \geqq 0. \tag{8}$$

To prove the converse, we first notice the following

Lemma 2. *Suppose that*

$$\sum_{\xi} a_{\xi} \zeta_{n+1}^{\xi} \equiv 0 \bmod. p^s, \qquad \xi \text{ in } U \bmod. U_n,$$

with a_{ξ} *in* Q_p. *Then, for any* ω *in* U,

$$\sum_{\xi}{}' a_{\xi} \equiv 0 \bmod. p^s,$$

where ξ *runs over all p-adic units* mod. U_n *such that* $\xi \equiv \omega \bmod. U_{n-1}$.[6]

The proof is elementary and, hence, is omitted here.

Now, assume that (8) holds for an odd index a and for any $n \geqq 0$. It then follows from (7) that

$$\sum_{\xi} (\sum_{\eta} s_n(\xi\eta^{-1})\eta^a) \zeta_{n+1}^{\xi} \equiv 0 \bmod. p^{n+2}.$$

By Lemma 2, we have, for any ω in U, that

$$\sum_{\xi}{}' \sum_{\eta} s_n(\xi\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+2}, \qquad \xi \equiv \omega \bmod. U_{n-1}. \tag{9}$$

Suppose that $n \geqq 1$ and put

$$\xi \equiv \omega + jp^n \bmod. p^{n+1}, \qquad 0 \leqq j < p.$$

Then,

$$s_n(\xi\eta^{-1}) = s_{n-1}(\omega\eta^{-1}) + kp^n, \qquad 0 \leqq k < p, \tag{10}$$

where k is determined by

$$k \equiv t_n(\omega\eta^{-1}) + j\eta^{-1} \bmod. p.$$

If ξ runs over p-adic units mod. U_n such that $\xi \equiv \omega \bmod. U_{n-1}$, k runs over all integers from 0 to $p-1$, and we obtain from (9) and (10) that

$$p \sum_{\eta} s_{n-1}(\omega\eta^{-1})\eta^a + p^n \sum_{k} \sum_{\eta} k\eta^a \equiv 0 \bmod. p^{n+2}.$$

Since $a \not\equiv 0 \bmod. p-1$, $\sum_{\eta} \eta^a = 0$ and it follows that

$$\sum_{\eta} s_{n-1}(\omega\eta^{-1})\eta^a \equiv 0 \bmod. p^{n+1}, \qquad n \geqq 1.$$

Thus, we see that (5) holds for any ξ in U and for any $n \geqq 0$, and the following result is proved:

---

[6] For $n = 0$, we understand $U_{-1} = 1$.

II. *The second coefficient* μ *in the formula* (1) *is positive if and only if there exists an odd integer* a, $1 \leqq a \leqq p-1$, *such that*

$$\sum_{\eta} \eta^a/(1-\zeta_{n+1}{}^{\eta}) \equiv 0 \bmod. p, \qquad \eta \in V, \tag{11}$$

for every $n \geqq 0$.

5. Let O_p be the ring of p-adic integers and $Q_p((x))$ the field of all power series in x with coefficients in Q_p. We denote by R the subring of those power series in $Q_p((x))$ which have coefficients in O_p, and by R_0 the subring of integral power series in R. Let $\alpha \neq 0$ be a non-unit integer in Ω_p. Then, for any $\phi = \phi(x)$ in R, the element $\phi(\alpha)$ in Ω_p is well defined and $\phi \to \phi(\alpha)$ gives a ring homomorphism of R into Ω_p. In particular, if $\alpha = 1-\zeta_{n+1}$, it induces a homomorphism of R_0 onto the ring of all integers in $Q_p(\zeta_{n+1})$.

Let a be an odd integer and η any element of V. The power series for $(1-x)^{\eta}$, defined in the usual way, is then contained in R_0 and we have

$$\eta^a/(1-(1-x)^{\eta}) = \eta^{a-1}/x + \phi_{\eta}(x),$$

with a power series ϕ_{η} in R_0. Putting $x = 1-\zeta_{n+1}$ in the above, it follows that

$$\sum_{\eta} \eta^a/(1-\zeta_{n+1}{}^{\eta}) = (1-\zeta_{n+1})^{-1} \cdot \sum_{\eta} \eta^{a-1} + \sum_{\eta} \phi_{\eta}(1-\zeta_{n+1}),$$

where $\phi_{\eta}(1-\zeta_{n+1})$ are integers in $Q_p(\zeta_{n+1})$.

Now, suppose that (11) holds for every $n \geqq 0$. The above equality then shows that $a \neq 1$ and that

$$\sum_{\eta} \phi_{\eta}(1-\zeta_{n+1}) \equiv 0 \bmod. p.$$

Using the fact that the elements $(1-\zeta_{n+1})^i$, $0 \leqq i < (p-1)p^n$, form a basis of the ring of integers in $Q_p(\zeta_{n+1})$ over O_p, it follows that

$$\sum_{\eta} \phi_{\eta}(x) \equiv 0 \bmod. pR_0 + x^{(p-1)p^n}R_0.$$

Since n is an arbitrary non-negative integer, we have then

$$\sum_{\eta} \phi_{\eta}(x) \equiv 0 \bmod. p,$$

and, consequently,

$$\sum_{\eta} \eta^a/(1-(1-x)^{\eta}) \equiv 0 \bmod. p.^{7}$$

Clearly, we can reverse the above argument and see that the above congruence conversely implies (11) for every $n \geqq 0$. Therefore:

---

[7] mod. p means mod. pR_0 or mod. pR.

III. *The second coefficient* μ *in the formula* (1) *is positive if and only if there exists an odd integer* a, $1 \leqq a \leqq p-1$, *such that*

$$\sum_{\eta} \eta^a/(1-(1-x)^{\eta}) \equiv 0 \bmod. p, \qquad \eta \in V. \tag{12}$$

Remark. III can be proved also by a different method using the classical formula for the second factor of the class number of K_n.

Now, if an element $\pi = \pi(x)$ of R_0 is of the form

$$\pi(x) = c_1 x + c_2 x^2 + \cdots, \qquad c_1 \in U,$$

there exists an automorphism of R over O_p which maps x to $\pi(x)$. Therefore, (12) is equivalent with

$$\sum_{\eta} \eta^a/(1-(1-\pi(x))^{\eta}) \equiv 0 \bmod. p, \tag{13}$$

for any such π. Choosing a suitable power series for œ, we can further transform the condition (12).

Consider the formal power series $L(x)$ and $E(x)$ defined by

$$L(x) = \sum_{i=0}^{\infty} x^{p^i}/p^i, \qquad E(x) = e^{-L(x)}.^{8}$$

As power series in $Q_p((x))$, they have the properties:

$$\eta L(x) = L(\eta x), \qquad E(x)^{\eta} = E(\eta x),$$

for any η in V. It is also known that $E(x)$ can be written in the form

$$E(x) = \prod_{m} (1-x^m)^{\mu(m)/m},$$

where $\mu(m)$ is the Mobius function and m runs over all positive rational integers prime to p. Hence $E(x)$ is contained in R_0 and it holds that

$$E(x) \equiv 1 - x \bmod. x^2 R_0.$$

Putting $\pi(x) = 1 - E(x)$ in (13), we then obtain

$$\sum_{\eta} \eta^a/(1-E(\eta x)) \equiv 0 \bmod. p.$$

Now, let $\sum_{k} a_k x^k$ be the power series for $(1-E(x))^{-1}$ and put

$$\psi_i(x) = \sum_{k \equiv i(p-1)} a_k x^k, \qquad 1 \leqq i \leqq p-1.$$

Then the left hand side of the above congruence is nothing but $(p-1)\psi_{p-a-1}(x)$ and we have immediately the following result:

---

[8] Cf. [1].

IV. *Let* $\psi_i(x)$ *be defined as above. Then the second coefficient* μ *in the formula* (1) *is positive if and only if there exists an odd integer* a, $1 \leqq a \leqq p-1$, *such that*

$$\psi_a(x) \equiv 0 \bmod. p.$$

The advantage of IV lies in that we can explicitly calculate $\psi_i(x)$, $1 \leqq i \leqq p-1$, by using the classical power series:

$$1/(1-e^{-z}) = 1/z + \tfrac{1}{2} - \sum_{n=1}^{\infty} (-1)^n B_n z^{2n-1}/(2n)\,!,$$

where B_n $(n \geqq 1)$ are the Bernoulli numbers. Put $z = L(x)$ in the above and notice that the exponents of x which appear in the power series $L(x)$ are always congruent with $1 \bmod. p-1$. We then obtain immediately that

$$\begin{aligned} \psi_{p-1}(x) &= \tfrac{1}{2}, & & \\ \psi_i(x) &= 0, & & 2 \mid i,\ i \neq p-1, \\ \psi_{p-2}(x) &= L(x)^{-1} - \textstyle\sum^{(p-2)} (-1)^n B_n L(x)^{2n-1}/(2n)\,!, & & \\ \psi_i(x) &= -\textstyle\sum^{(i)} (-1)^n B_n L(x)^{2n-1}/(2n)\,!, & & 2 \nmid i,\ i \neq p-2, \end{aligned}$$

where $\sum^{(i)}$ means the summation over all $n \geqq 1$ such that $2n-1 \equiv i \bmod. p-1$.

Now, it is clear from the above that $\psi_{p-2}(x) \not\equiv 0 \bmod. p$.[9] For an odd $a \neq p-2$, we can then calculate the coefficients of $x^{a+k(p-1)}$, $k \geqq 0$, in $\psi_a(x)$ from the last equality and, putting them to be congruent to $0 \bmod. p$, we obtain a sequence of congruence relations on the Bernoulli numbers which altogether form an equivalent condition with $\psi_a(x) \equiv 0 \bmod. p$. For instance, we obtain from the first two coefficients the following congruences:

$$\begin{aligned} &B'(\tfrac{1}{2}(a+1)) \equiv 0 \bmod. p, \\ &B'(\tfrac{1}{2}(a+1)) \equiv B'(\tfrac{1}{2}(a+1) + \tfrac{1}{2}(p-1)) \bmod. p^2, \end{aligned}$$

where $B'(n)$ is defined by

$$B'(n) = (-1)^n B_n/n, \qquad n \geqq 1.$$

The first congruence in the above shows that if $\mu > 0$, i.e., if $\psi_a(x) \equiv 0 \bmod. p$ for some odd a, p must be an irregular prime. But this can be otherwise proved easily without making use of the above result.

For the irregular primes $p = 37, 59, 67$, we can determine the index a for which the first congruence is satisfied, and then see that the second congruence does not hold for such an a.[10] Hence, we have $\mu=0$ for these prime numbers. However, in these cases, it is also known that the order of $G(L_1/K_1)$ is p^2 and, by the structural theorem on Γ-groups,[11] we can prove more precisely that $G(L/K)$ is isomorphic with Γ and that $\lambda=1$, $\mu=0$ and $\nu=0$.

---

[9] This corresponds to the fact that (5), (11) and (12) do not hold for $a = 1$.

Remark. Using the fact that the coefficients of the power series for $(1-E(x))^{-1}$ are always p-adic integers, we can obtain, by a similar argument as above, various congruence relations for the Bernoulli numbers mod. p^n.

THE INSTITUTE FOR ADVANCED STUDY
AND THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] E. Artin and H. Hasse, "Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln," *Abhandlungen aus dem Mathematischen Seminar der Hamburg Universität*, vol. 6 (1928), pp. 146-162.

[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin, 1952.

[3] D. Hilbert, "Die Theorie der algebraischen Zahlkörper," *Jahresbericht der Deutschen Mathematiker-Vereinigung*, vol. 4 (1897), pp. 175-546.

[4] K. Iwasawa, "On Γ-extensions of algebraic number fields," to appear shortly in *Bulletin of the American Mathematical Society.*

[5] R. E. MacKenzie, "Class group relations in cyclotomic fields," *American Journal of Mathematics*, vol. 74 (1952), pp. 759-763.

[6] F. Pollaczek, "Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln," *Mathematische Zeitschrift*, vol. 21 (1924), pp. 1-38.

[7] T. Takagi, "Zur Theorie der Kreiskörpers," *Journal für die reine und angewandte Mathematik*, vol. 157 (1927), pp. 230-238.

---

[10] Cf. [6].

[11] Cf. [4], § 5.

ON A THEOREM OF TORELLI.*[1]

By T. Matsusaka.

Let Γ be a complete non-singular surve, J^g be its Jacobian variety and α be the canonical mapping of Γ into J. Let θ be a *canonical divisor on J with respect to* Γ, which is determined uniquely up to translations. By means of $\mathfrak{L}(m\theta)$, we can embed J into a projective space, i. e. $m\theta$ is *linearly effective*, whenever m is sufficiently large (cf. Weil [8]). Therefore, the set $\mathfrak{X}$ of positive divisors X on J, such that $s\theta \equiv tX \bmod G_n(J)$ for two positive integers s and t, defines a *structure of polarization* on J (cf. Weil [9], Matsusaka [4]). When J is polarized this way, we call it the *canonically polarized Jacobian variety with respect to* Γ. The purpose of this paper is to show that when two canonically polarized Jacobian varieties are isomorphic, then two curves are isomorphic. First this theorem was proved by Torelli (Torelli [5]) in the classical case and another proof was given recently by Andreotti also in the classical case (Andreotti [1]). Quite recently, A. Weil showed that Andreotti's idea can be generalized to the abstract case (Weil [10]). The present author will show that Torelli's idea can also be generalized to the abstract case.

Let C be another complete non-singular curve, J'^g be the Jacobian variety of C and α' be the canonical mapping of C into J'. Let θ' be a canonical divisor on J' with respect to C and $\mathfrak{X}'$ be the set of positive J'-divisors which defines the canonical polarization on J' with respect to C. Let us assume that there is an isomorphism β between two thus polarized Jacobian varieties. Then β must be an isomorphism of the underlying Jacobian varieties satisfying $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Therefore, we make the following identification hereafter: we identify α' with $\beta^{-1}\cdot\alpha'$ and J' with J. Then J is the Jacobian variety of Γ, and at the same time, the Jacobian variety of C; moreover, canonical divisors θ and θ' on J with respect to Γ and C satisfy $\theta \equiv \theta' \bmod G_n(J)$. When that is so, there is a point d on J such that $\theta' = \theta_d$ by Weil [7], Cor. 2, Th. 32. We fix a common field k of definition for $\Gamma, C, J, \alpha, \alpha', \theta, d$ and regard k as a *basic field. All fields we shall consider shall be assumed to contain k.*

---

* Received February 14, 1958.

[1] We shall follow the same terminology and conventions as in [4], [6] and [7].

We shall denote by W^r (resp. V^r) the locus of $\sum_1^r \alpha(x_i)$ (resp. $\sum_1^r \alpha'(y_i)$) over k, where $(x_1,\cdots,x_r)$ (resp. $(y_1,\cdots,y_r)$) is a set of r independent generic points of Γ (resp. C) over k. We assume that $W^{g-1}=\theta$, $V^{g-1}=\theta'$. We have $W^1=\alpha(\Gamma)$, $V^1=\alpha'(C)$; we shall write W for W^{g-2} and V for V^{g-2}. Let $\mathfrak{k}$ and $\mathfrak{k}'$ be rational canonical divisors of Γ and C respectively over k. Denoting by δ the identity automorphism of J, $-\delta+S(\alpha(\mathfrak{k}))$ leaves θ invariant, and also $-\delta+S(\alpha'(\mathfrak{k}'))$ leaves θ' invariant (cf. Weil [7], Prop. 19). Let U be any subvariety of J, then we shall denote by U^- the transform of U by $-\delta$. We shall denote by W^* (resp. V^*) the transform of W (resp. V) by $-\delta+S(\alpha(\mathfrak{k}))$ (resp. $-\delta+S(\alpha'(\mathfrak{k}'))$).

Let now A be an arbitrary Abelian variety and X, Y be two subvarieties of A. Let x and y be independent generic points of X and Y over a common field of definition K for X and Y. We shall denote by $X\oplus Y$ the locus of $x+y$ over K. This definition can be extended to a finite set of positive A-cycles by linearity.

1. LEMMA 1. *$W_{\alpha(x)}$ and $W^*_{-\alpha(x)}$ are subvarieties of θ for all x on Γ. When x is a generic point of Γ over k, then $W_{\alpha(x)}$ and $W^*_{-\alpha(x)}$ contain generic points of θ over k.*

Proof. $W_{\alpha(x)}$ is a subvariety of θ by the definitions of W and θ. Since θ is invariant by the automorphism $-\delta+S(\alpha(\mathfrak{k}))$ of the underlying variety of J, $W^*_{-\alpha(x)}$ is also a subvariety of θ. By the same reason as above, when $W_{\alpha(x)}$ contains a generic point of θ over k, then so does $W^*_{-\alpha(x)}$. Assume now that x is a generic point of Γ over k, and let $w=\sum_1^{g-2}\alpha(x_i)$ be a generic point of W over $k(x)$. Then $(x,x_1,\cdots,x_{g-2})$ is a set of independent generic points of Γ over k; hence $w+\alpha(x)$ is a generic point of θ over k. Our lemma is thereby proved.

LEMMA 2. *Let U be a subvariety of co-dimension 1 on θ and w be a point of W. Then $U\cap\alpha(\Gamma)_w\neq\phi$.*

Proof. Let K be a field of definition for U and u be a generic point of U over K. Then u can be written uniquely as $u=\sum_1^{g-1}\alpha(x_i)$, where the x_i are points on Γ, otherwise $U\oplus\alpha(\Gamma)$ is a subvariety of W^* (cf. Weil [7], Prop. 16), which is a contradiction since $\dim U\oplus\alpha(\Gamma)=g-1$. We can find a set of $g-2$ independent generic points of Γ over K, say $(x_1,\cdots,x_{g-2})$, from the set $(x_1,\cdots,x_{g-1})$. Put $w=\sum_1^{g-2}\alpha(x_i)$, then w is a generic point of W over K. $\alpha(\Gamma)_w$ is a subvariety of θ and contains u. Hence $\alpha(\Gamma)_w\cap U$ is not empty, and from this our lemma follows immediately.

LEMMA 3. i) *Let D be a curve on J; then $D_t \cap V^*$ is not empty if and only if t is a point of $V^* \oplus D^-$.* ii) *$\alpha(\Gamma)_t$ is a subvariety of $\theta'_{\alpha'(y)}$ with y on C if and only if t is a point of $W_{d+\alpha'(y)}$.* iii) *$W_d \oplus \alpha'(C) = V^* \oplus \alpha(\Gamma)^-$.*

Proof. Let $S(\alpha'(\mathfrak{t}')) - v$ be a point in $D_t \cap V^*$. There is a point x on D such that $t = S(\alpha'(\mathfrak{t}')) - v - x$, which shows that t is on $V^* \oplus D^-$. Conversely, if t is on $V^* \oplus D^-$, then D_t and V^* have clearly a point in common. i) is thereby proved.

Assume that $\alpha(\Gamma)_t$ is on $\theta'_{\alpha'(y)}$. Since $\theta' = \theta_d$, $\alpha(\Gamma)_{t-d-\alpha'(y)}$ is contained in θ. By Weil [7], Th. 20, $\alpha(\Gamma)_{t-d-\alpha'(y)}$ is contained in θ if and only if $\alpha'(y) + d - t$ is on W^-. Therefore it is contained in θ if and only if t is a point of $W_{d+\alpha'(y)}$. ii) is thereby proved.

By our Lemma 1, $V^*_{-\alpha'(y)}$ is a subvariety of $\theta' = \theta_d$ for all y on C; hence $V^*_{-\alpha'(y)-d}$ is a subvariety of θ for all y on C. If we show that V^* and $\alpha(\Gamma)_{w+d+\alpha'(y)}$ have non-empty intersection for all w on W and y on C, then $W_d \oplus \alpha'(C)$ is contained in $V^* \oplus \alpha(\Gamma)^-$; and when that is so, we have $W_d \oplus \alpha'(C) = V^* \oplus \alpha(\Gamma)^-$ since both have the same dimension. Since $\alpha(\Gamma)_{w+d+\alpha'(y)} \cap V^* \neq \phi$ and $\alpha(\Gamma)_w \cap V^*_{-d-\alpha'(y)} \neq \phi$ imply each other, iii) follows from our Lemma 2.

2. Let X^r be the subvariety of $W^r \times \Gamma$ defined over k, defined by the following conditions: Let w be a generic point of W^r over k, then $X(w) = \mathfrak{m}$ is a positive Γ-divisor, $\deg(\mathfrak{m}) = r$ and $S(\alpha(\mathfrak{m})) = w$ (cf. Weil [7], Th. 18 and Weil [6], Chap. VII, Th. 12). We are going to study some properties of X when $r = g$ and $r = g - 1$. Whenever D is a curve on W^r such that $X^r \cdot (D \times \Gamma)$ is defined, we write

$$(D \times \Gamma) \cdot X = T + \mathfrak{a} \times \Gamma + D \times \mathfrak{b},$$

where every component of T has the projection D on D and Γ on Γ. We have obviously $\deg(\mathfrak{b}) \leqq r$ from the definition of X.

LEMMA 4. *Let t be a point on J. Then $(t \times \Gamma) \cdot X^g$ is defined on $J \times \Gamma$ if and only if t is not a point of W^*. Let D be a curve on J. Then $(D_t \times \Gamma) \cdot X^g$ is defined on $J \times \Gamma$ if and only if D_t is not a subvariety of W^*.*

Proof. If t is not a point of W^*, then denoting by v a generic point of J over k, $X(v)$ has the uniquely determined specialization $\mathfrak{m}$ over $v \rightarrow t$ ref. k, since $S(\alpha(\mathfrak{m}))$ must be t (cf. Weil [7], Prop. 16). Hence $(t \times \Gamma) \cdot X$ is defined. Conversely, if t is a point of W^*, then for any point x on Γ, there is a positive Γ-divisor $\mathfrak{m}$ of degree g such that $\mathfrak{m} - x \succ 0$ and that $S(\alpha(\mathfrak{m})) = t$. When that is so, it is easy to see that $(X(v), v) \rightarrow (\mathfrak{m}, t)$ ref. k and this implies that $(t \times \Gamma) \cdot X$ is not defined.

Assume that D_t is not contained in W^*; then the preceding result shows that $D_t \times \Gamma$ cannot be contained in X. Hence $(D_t \times \Gamma) \cdot X$ is defined since X is a divisor on $J \times \Gamma$. On the other hand, if D_t is a subvariety of W^*, $u \times \Gamma$ is contained in X for any point u on D_t. Therefore $(D_t \times \Gamma) \cdot X$ is not defined, and our Lemma is thereby proved.

LEMMA 5. *Let D be a curve on J and u be a point on J such that $(D_u \times \Gamma) \cdot X^g$ is defined.* (i) *A point t on D_u is a component of $\mathfrak{a}$ if and only if it is a component of $D_u \cap W^*$. When $D = \alpha'(C)$, then $\mathfrak{a} \neq 0$ if and only if $\mathfrak{b} \neq 0$.* (ii) *When u is a generic point of J over a field K over which D is defined, then $\mathfrak{a} = 0$.* (iii) *Assume that $D = \alpha'(C)$ and let x be a generic point of Γ over $K(u)$. If we put $\mathfrak{n} = {}^tT(x) + \mathfrak{a}$, we have*

$$S(\alpha(\mathfrak{n})) = \alpha(x) + (g-1)u + S(\alpha'(\mathfrak{f}')) - d.$$

Proof. Let t be a component of $\mathfrak{a}$. Then $(t \times \Gamma) \cdot X$ is not defined and t is a point of W^* by Lemma 4. Conversely, if t is a point in $D_u \cap W^*$, then $t \times \Gamma$ is contained in X by Lemma 4, which shows that t is a component of $\mathfrak{a}$. When $D = \alpha'(C)$, $D_u \cap W^* \neq \phi$ and $D_u \subset \theta_{\mathfrak{a}(x)}$, for a certain x on Γ, are equivalent by Lemma 3. (i) is thereby proved.

When u is a generic point of J over K, u is not a point of $W^* \oplus D^-$. Hence D_u and W^* have no common point by Lemma 3, and $\mathfrak{a} = 0$; (ii) is thereby proved.

We have

$$(1) \quad (((\alpha'(C)_u \times \Gamma) \cdot X) \cdot (\alpha'(C)_u \times x))_{\alpha'(C) \times \Gamma} = ((\alpha'(C)_u \times \Gamma) \cdot X) \cdot (J \times x)$$
$$= ((\alpha'(C)_u \times \Gamma) \cdot (X \cdot (J \times x)) = (\alpha'(C)_u \times \Gamma) \cdot (\theta_{\mathfrak{a}(x)} \times x) = \alpha'(C)_u \cdot \theta_{\mathfrak{a}(x)} \times x$$

by Weil [6], Chap. VII, Cor., Th. 18, Chap. VII, Th. 10, and Chap. VI, Th. 11. Hence

$$\begin{aligned} S(\alpha(\mathfrak{n})) = S(\alpha'(C)_u \cdot \theta_{\mathfrak{a}(x)}) &= g \cdot u + S(\alpha'(C) \cdot \theta'_{-d+\mathfrak{a}(x)-u}) \\ &= (g-1) \cdot u - d + \alpha(x) + S(\alpha'(\mathfrak{f}')) \end{aligned}$$

by Weil [7], Th. 20. (iii) is thereby proved.

LEMMA 6. *$(\alpha'(C)_u \times \Gamma) \cdot X^g$ is defined if and only if $\alpha(\Gamma)_{-u-d}$ is not contained in $V^- = V^*_{-S(\alpha'(\mathfrak{f}'))}$, and when that is so, a point x of Γ is a component of $\mathfrak{b}$ if and only if $\alpha(x)$ is a component of $\alpha(\Gamma) \cap V^-_{u+d}$. In other words, x on Γ is a component of $\mathfrak{b}$ if and only if*

$$\alpha(x) + (g-1) \cdot u + S(\alpha'(\mathfrak{f}')) - d \in V^*_{g \cdot u}.$$

Proof. First, let us show that $\alpha'(C)_u \times x$ is contained in X if and only if $\alpha(x) \in V^-_{u+d}$. By the formula (1), we have

$$\alpha'(C)_u \times \Gamma \cap X \cap \alpha'(C)_u \times x = (\alpha'(C)_u \cap \theta_{\mathfrak{a}(x)}) \times x.$$

Hence $\alpha'(C)_u \times x$ is contained in X if and only if $\alpha'(C)_u \subset \theta_{\alpha(x)}$. $\alpha'(C)_u$ is a subvariety of $\theta_{\alpha(x)}$ if and only if u is on $V_{-d+\alpha(x)}$ by (ii), Lemma 3. u is a point of $V_{-d+\alpha(x)}$ if and only if $\alpha(x)$ is a point of $V^{-}{}_{u+d}$, and our assertion is proved.

$(\alpha'(C)_u \times \Gamma) \cdot X$ is defined if and only if $\alpha'(C)_u \times \Gamma$ is not contained in X and this is so if and only if $\alpha(\Gamma)$ is not contained in $V^{-}{}_{u+d}$ by what we have observed. Our lemma is thereby proved.

LEMMA 7. *Let* Γ *be non-hyperelliptic,* U *be a subvariety of* W^* *and assume that* U *contains a generic point of* W^* *over* k. *Let* K *be a field of definition for* U *and* x *be a generic point of* Γ *over* K. *Then* $X^{g-1} \cdot (U_{-\alpha(x)} \times \Gamma)$ *is defined and can be written as* $T + U_{-\alpha(x)} \times \mathfrak{q}(x) + Y$, *where every component of* T *has the projection* $U_{-\alpha(x)}$ *on* $U_{-\alpha(x)}$ *and* Γ *on* Γ *and the projection of every component of* Y *on* $U_{-\alpha(x)}$ *is a proper subvariety of* $U_{-\alpha(x)}$. *Then there is an irrational pencil* Σ, *free from fixed components, defined over* K *on* Γ *such that* $x + \mathfrak{q}(x) = m \cdot \mathfrak{p} + \mathfrak{c}$, *where* m *is a positive integer,* $\mathfrak{p}$ *is a generic member of* Σ *over* K *and* $\mathfrak{c}$ *is a positive rational divisor of* Γ *over* K.

Proof. Since U is a subvariety of W^*, it follows that $U_{-\alpha(x)}$ is a subvariety of θ by Lemma 1. Moreover, since U contains a generic point of W^* over k, it follows that $U_{-\alpha(x)}$ contains a generic point of θ over k by Lemma 1. It is clear that $X^{g-1} \cdot (U_{-\alpha(x)} \times \Gamma)$ is defined and that $x + \mathfrak{q}(x)$ is rational over $K(x)$. Let x' be a generic point of Γ over K and put $X \cdot (U_{-\alpha(x')} \times \Gamma) = T' + U_{-\alpha(x')} \times \mathfrak{q}(x') + Y'$. Let s be a generic point of U over $K(x, x')$. Then we have

$$s = S(\alpha(T(s - \alpha(x)) + \mathfrak{q}(x) + x)) = S(\alpha(T'(s - \alpha(x')) + \mathfrak{q}(x') + x')),$$

and therefore, we have

$$T(s - \alpha(x)) + \mathfrak{q}(x) + x \sim T'(s - \alpha(x')) + \mathfrak{q}(x') + x'$$

by Weil [7], Th. 19. Since s is a generic point of W^* over k by our assumption, it follows that $l(T(s - \alpha(x)) + \mathfrak{q}(x) + x) = 2$ by Lemma 1, Appendix; since $\mathfrak{L}(T(s - \alpha(x)) + \mathfrak{q}(x) + x)$ is defined over the algebraic closure of $K(s)$, and since x is a generic point of Γ over $K(s)$, it follows that the divisor $T(s - \alpha(x)) + \mathfrak{q}(x) + x$ is a generic divisor of $\mathfrak{L}(T(s - \alpha(x)) + \mathfrak{q}(x) + x)$ over $\overline{K(s)}$. Assume that x' is a component of $\mathfrak{q}(x) + x$, which is not algebraic over K. Then x' is a generic point of Γ over $K(s)$ and therefore

$$T(s - \alpha(x)) + \mathfrak{q}(x) + x = T'(s - \alpha(x')) + \mathfrak{q}(x') + x'.$$

$K(x)$ and $K(x')$ have the same algebraic closure $\overline{K(x)}$, $T(s - \alpha(x))$ and

$T'(s-\alpha(x'))$ consist of generic points of Γ over $\overline{K(x)}$ and $\mathfrak{q}(x)+x$, $\mathfrak{q}(x')+x'$ are both rational over $\overline{K(x)}$. Therefore $x+\mathfrak{q}(x)=x'+\mathfrak{q}(x')$. Let z be the Chow-point of $x+\mathfrak{q}(x)$; z is rational over $K(x)$ and hence z has a locus Z over K. Let f be the rational mapping of Γ onto Z such that $f(x)=z$. When x' is a component of $x+\mathfrak{q}(x)$, which is not algebraic over K, then $f(x')=z$ by what we have seen. Hence $x+\mathfrak{q}(x)=m\cdot f^{-1}(z)+\mathfrak{c}$, where m is a positive integer and $\mathfrak{c}$ is a fixed rational divisor over K (cf. Weil [6], Chap. VI, Th. 11).

In order to complete our lemma, it is sufficient to prove that Z is not a rational curve. If Z is a rational curve, then $x+\mathfrak{q}(x)\sim x'+\mathfrak{q}(x')$ whenever x and x' are two independent generic points of Γ over K. Therefore $T(s-\alpha(x))\sim T'(s-\alpha(x'))$. Since $U_{-\alpha(x)}$ contains a generic point of θ over k, $s-\alpha(x)$ is a generic point of θ over k and consequently $T(s-\alpha(x))+\mathfrak{q}(x)$ is a generic divisor on Γ of degree $g-1$ over k. Hence $T(s-\alpha(x))\sim T'(s-\alpha(x'))$ if and only if $T(s-\alpha(x))=T'(s-\alpha(x'))$. When x and x' are independent generic points of Γ over $K(s)$, then $T(s-\alpha(x))+\mathfrak{q}(x)+x$ and $T'(s-\alpha(x'))+\mathfrak{q}(x')+x'$ are two independent generic divisors of the pencil $\mathfrak{L}(T(s-\alpha(x))+\mathfrak{q}(x)+x)$ over the algebraic closure of $K(s)$. Therefore, if $T(s-\alpha(x))=T'(s-\alpha(x'))$, then $T(s-\alpha(x))$ is a fixed divisor of the pencil, which is contrary to our hypothesis that Γ is not hyperelliptic (cf. Lemma 1, Appendix). Our lemma is thereby proved.

3. LEMMA 8. *Let t and u be generic points of $W^*\oplus\alpha'(C)^-$ and $W^*\oplus\alpha'(C)$ over k. Put $(\alpha'(C)_t\times\Gamma)\cdot X^g=T+\alpha'(C)_t\times\mathfrak{b}+\mathfrak{a}\times\Gamma$, and also*

$$(\alpha'(C)^-_u\times\Gamma)\cdot X^g=T'+\alpha'(C)^-_u\times\mathfrak{b}'+\mathfrak{a}'\times\Gamma.$$

When Γ is not a hyperelliptic curve, either $\deg(\mathfrak{b})=1$ *or* $\deg(\mathfrak{b}')=1$.

Proof. By Lemmas 3 and 6, $\mathfrak{b}$ and $\mathfrak{b}'$ are not 0. Assume that $\deg(\mathfrak{b})>1$. Write $\mathfrak{k}=\sum_1^s c_i$ and put $v=S(\alpha(\mathfrak{k}))-t+\alpha(c_{s-1})+\alpha(c_s)$. $\alpha'(C)^-_v$ contains a generic point of W^* over k an dis contained in it. In fact, putting $K=\overline{k(t)}$, a generic point of $\alpha'(C)_t$ over K is a generic point of J over k. Therefore, when we write a generic point of $\alpha'(C)_t$ over K in the form

$$S(\alpha(\textstyle\sum_1^{g-s}(x_i)+\sum_1^s(c_i))),$$

$(x_1,\cdots,x_{g-s},c_1,\cdots,c_s)$ is a set of g independent generic points of Γ over k. When that is so, $S(\alpha(\mathfrak{k}-\sum_1^{g-s}(x_i)-\sum_1^{s-2}(c_i)))$ is a generic point of W^* over k by the definition of W^*. Our assertion is thereby proved.

Let y_1 and y_2 be two independent generic points of Γ over K. Put $z = v - \alpha(y_1) + \alpha(y_2)$ and

$$(\alpha'(C)^{-}_{z} \times \Gamma) \cdot X^{g} = T'' + \alpha'(C)^{-}_{z} \times \mathfrak{b}'' + \mathfrak{a}'' \times \Gamma.$$

We shall show that $\mathfrak{b}'' = y_2$, which is sufficient to prove our lemma (cf. Lemmas 3 and 6). Since $\alpha'(C)^{-}_{v}$ contains a generic point of W^* over k and is contained in it, we may apply Lemma 7 to this curve. Let $\bar{X}$ be the subvariety X^{g-1} on $\theta \times \Gamma$ defined in no. 2. Since $\alpha'(C)^{-}_{v-\alpha(y_1)}$ contains a generic point of θ over K and is contained in it by Lemma 1, $\alpha'(C)^{-}_{v-\alpha(y_1)} \times \Gamma$ is not a subvariety of $\bar{X}$. Therefore $\bar{X} \cdot (\alpha'(C)^{-}_{v-\alpha(y_1)} \times \Gamma)$ is defined. Put

$$\bar{X} \cdot (\alpha'(C)^{-}_{v-\alpha(y_1)} \times \Gamma) = \bar{T} + \alpha'(C)^{-}_{v-\alpha(y_1)} \times \mathfrak{b} + \mathfrak{a} \times \Gamma,$$

and $\mathfrak{b} = \mathfrak{q}(y_1)$. Let $\mathfrak{S}$ be the set of specializations of $y_1 + \mathfrak{q}(y_1)$ over K, then by our Lemma 7, $\mathfrak{S}$ is an irrational pencil. Next, we claim that $\mathfrak{S}$ is free from fixed components. Let r be a generic point of $\alpha'(C)^{-}_{v}$ over $K(y_1)$, then $r = S(\alpha(\bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1))$. Since r is a generic point of W^* over k and since

$$\deg(\bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1) = g,$$

$\mathfrak{m} = \bar{T}(r - \alpha(y_1)) + \mathfrak{q}(y_1) + y_1$ is a generic divisor of $\mathfrak{L}(\mathfrak{m})$ over the algebraic closure of $K(r)$. Since $\mathfrak{L}(\mathfrak{m})$ has no fixed component by Lemma 1, Appendix, it follows that $\mathfrak{q}(y_1)$ cannot contain a component which is algebraic over $K(r)$. Hence our assertion is proved.

By Lemma 3, Appendix, $\mathfrak{S}$ is defined over $\bar{k}$, and hence $S(\alpha(\mathfrak{q}(y_1) + y_1)) = a$ is a constant, which is independent with respect to v over k. Assume that $\mathfrak{q}(y_1)$ is not empty, then $\deg(y_1 + \mathfrak{q}(y_1)) = m > 1$ and $\alpha'(C)^{-}_{v}$ is contained in $W^{g-m}{}_{a}$. Since $\alpha'(C)^{-}_{v}$ contains a generic point of W^* over k, we must have $m \leqq 2$. When $m = 2$, we have $W^{g-2}{}_{a} = W^*$ and this is possible if and only if $l(y_1 + \mathfrak{q}(y_1)) > 1$ by the theorem of Riemann-Roch. This contradicts our hypothesis that Γ is not a hyperelliptic curve. Thus $m = 1$ and $\mathfrak{q}(y_1) = 0$. From this we see immediately that $\mathfrak{b}'' = \alpha(y_2)$ and our lemma is thereby proved.

4. THEOREM (hyperelliptic case). *Let Γ and C be two complete non-singular hyperelliptic curves of genus g. Let J (resp. J') be the Jacobian variety of Γ (resp. C) and α (resp. α') be the canonical mapping of Γ (resp. C) into J (resp. J'). Assume that there is an isomorphism of β of J into J' such that canonical divisors θ and θ' on J and J' with respect to Γ*

and C satisfy $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Then there is a birational transformation h of Γ onto C such that

$$\alpha' \cdot h = \pm \beta \cdot \alpha + \textit{constant};$$

we can select $+$ or $-$ arbitrarily, but if it is once selected, h and the constant are uniquely determined by β.

Proof. We make the identification stated in the beginning of this paper. Let $\mathfrak{c}$ (resp. $\mathfrak{c}'$) be a positive divisor of degree 2 on Γ (resp. C) such that $l(\mathfrak{c})$ (resp. $l(\mathfrak{c}')$) > 1. Since $\theta' = \theta_d$, we may assume that $\theta = \theta'$ by adding a suitable constant to α'. By the proposition in our Appendix, a point u of θ is a singular point of θ if and only if a positive Γ-divisor $\mathfrak{m}$ of degree $g-1$ such that $S(\alpha(\mathfrak{m})) = u$ satisfies $l(\mathfrak{m}) > 1$. When that is so, $l(\mathfrak{m} - \mathfrak{c})$ is positive and this shows that u is a point of $W^{g-3}{}_s$, where $s = S(\alpha(\mathfrak{c}))$. Conversely, it is clear that any point of $W^{g-3}{}_s$ is a singular point of θ by the same proposition. When we put $s' = S(\alpha'(\mathfrak{c}'))$, $V^{g-3}{}_{s'}$ is also the set of singular points of $\theta' = \theta$ and hence we have $W^{g-3}{}_s = V^{g-3}{}_{s'}$.

It is easy to see that $W^* = W^{g-2}{}_s$, $V^* = V^{g-2}{}_{s'}$ (cf. Weil [7], Prop. 16). Let t be a generic point of $W^* \oplus \alpha'(C)^-$ over $K = k(s, s')$. By Lemma 3, t can be written as $v + \alpha(x)$, where v and x are independent generic points of V and Γ over K. By the same lemma, $\alpha'(C)_v \cap W^*{}_{-\alpha(x)}$ is not empty. *We shall show that it contains at least $g-1$ distinct points.* A generic point of $W^*{}_{-\alpha(x)}$ over $K(x)$ can be written as $S(\alpha'(\sum_1^{g-1} y_i))$ where the y_i are points on C, and $g-2$ points among $(y_1, \cdots, y_{g-1})$, say $(y_1, \cdots, y_{g-2})$, are independent generic points of C over $K(x)$. Put $v' = S(\alpha'(\sum_1^{g-2} y_i))$; then v' is a generic point of V over $K(x)$ and $\alpha'(C)_{v'}$ contains a generic point of θ over K, which is a generic point of $W^*{}_{-\alpha(x)}$ over $K(x)$. Since v and v' are generic specializations of each other over $K(x)$, $\alpha'(C)_v$ also has the same properties. Hence $\alpha'(C)_v \cdot W^*{}_{-\alpha(x)}$ is defined on θ and is not empty. Identifying v and v', let y'_i be the point on C such that $y_i + y'_i \sim \mathfrak{c}'$. Then $\alpha'(y'_i) + v$ is on $\alpha'(C)_v$ and $V^{g-3}{}_{s'} = W^{g-3}{}_s$. Thus $\alpha'(y'_i) + v = S(\alpha(\mathfrak{m}_i))$, where $\mathfrak{m}_i$ is a positive Γ-divisor of degree $g-1$; since $l(\mathfrak{m}_i) > 1$, $\mathfrak{m}_i \sim x' + \mathfrak{n}_i$, where x' is the point on Γ such that $x + x' \sim \mathfrak{c}$ and $\mathfrak{n}_i$ is a positive Γ-divisor of degree $g-2$. It follows that $\alpha'(y'_i) + v \in W^{g-2}{}_{\alpha(x')} = W^*{}_{-\alpha(x)}$. It is clear that when $i \neq j$, $\alpha'(y'_i) + v \neq \alpha'(y'_j) + v$. $\alpha'(y'_i) + v$ is a singular point of θ by the proposition in our Appendix. Thus our assertion is proved.

Since t is a generic point of $W^* \oplus \alpha'(C)^-$ over K, $\alpha'(C)_t$ is not contained in W^*. Therefore $(\alpha'(C)_t \times \Gamma) \cdot X^g$ is defined and can be written in the form $T + \mathfrak{a}' \times \Gamma + \alpha'(C)_t \times \mathfrak{b}$. By (i), Lemma 5, we have $\deg(\mathfrak{a}') \geqq g-1$. If $\deg(\mathfrak{a}') = g$, then $T=0$, $\deg(\mathfrak{b}) = g$ by the formula (1) and this is impossible from the definition of X and Weil [7], Th. 19. Hence we must have $\deg(\mathfrak{a}') = g-1$, and since $(\alpha(C)_t \times \Gamma) \cdot X$ is a correspondence of type (g, g) by the formula (1), it follows that T is the graph of a rational mapping $\bar{h}$ of Γ onto $\alpha'(C)_t$. Since a generic point $\alpha'(y) + t$ of $\alpha'(C)_t$ over $K(t)$ is a generic point of J over K, every component of $T(\alpha'(y)+t)$ has the coefficient 1, which proves that $\bar{h}$ is a separable mapping. By Lemma 2, Appendix, $\bar{h}$ is then a birational transformation, and we have $\alpha'(y) + t = \alpha(\bar{h}^{-1}(\alpha'(y)+t)) + S(\alpha(\mathfrak{b}))$. Thus we see that $\alpha'(C) = \alpha(\Gamma)_c$, where c is a constant, and that there is a birational transformation h of Γ onto C such that $\alpha(x) = \alpha'(h(x)) + c'$, where c' is a constant. Let f' be the birational transformation of C onto itself such that whenever y is a point of C, $y + f'(y) \sim \mathfrak{c}'$. Then since $\alpha'(h(x)) + \alpha'(f' \cdot h(x)) = S(\alpha'(\mathfrak{c}'))$, we see that $\alpha(x) = -\alpha'(f' \cdot h(x)) + c''$, where c'' is a constant. Since $\mathfrak{L}(\mathfrak{c})$ is uniquely determined on Γ, h is determined uniquely by the relation $\alpha = \alpha' \cdot h + \text{constant}$; in the same way, $f' \cdot h$ is uniquely determined by the relation $\alpha = -\alpha' \cdot (f' \cdot h) + \text{constant}$. Our theorem is thereby proved.

THEOREM (non-hyperelliptic case). *Let Γ and C be two complete non-singular curves of the same genus g and assume that one of the two curves is not a hyperelliptic curve. Let J (resp. J') be the Jacobian variety of Γ (resp. C) and α (resp. α') be the canonical mapping of Γ (resp. C) into J (resp. J'). Assume that there is an isomorphism β of J onto J' such that canonical divisors θ and θ' on J and J' with respect to Γ and C satisfy $\beta(\theta) \equiv \theta' \bmod G_n(J')$. Then there is a birational transformation h of Γ to C such that*

$$\alpha' \cdot h = \pm \beta \cdot \alpha + \textit{constant},$$

where the signature, h and the constant are uniquely determined by β.

Proof. As in the proof of the preceding theorem, we make the identification $J = J'$, as stated in the beginning of this paper. For the sake of simplicity, let us assume that Γ is not hyperelliptic. Then by Lemma 8, either $\alpha'(C)$ or $\alpha'(C)^-$ satisfies the property described in the Lemma. Assume that $\alpha'(C)$ satisfies it, i.e. letting t be a generic point of $W^* \oplus \alpha'(C)^-$ over k, and writing $(\alpha'(C)_t \times \Gamma) \cdot X^g = T + \mathfrak{a}' \times \Gamma + \alpha'(C)_t \times \mathfrak{b}$, assume that $\deg(\mathfrak{b}) = 1$. By Lemma 6, when we put $v = -t - d + S(\alpha'(\mathfrak{k}'))$, $\alpha(\Gamma)_v$ and V^* have just a single point in common. Then v is a generic point of $V^* \oplus \alpha(\Gamma)^- = W_d \oplus \alpha'(C)$ over k by Lemma 3, and can be written as $v = w + \alpha'(y) + d$, where w and y are independent generic points of W and

C over k. Thus we see that $V^*_{-\alpha'(y)}$ and $\alpha(\Gamma)_{w+d}$ have just a single point in common. It is easy to see that we have

$$\theta' \cap \theta'_{\alpha'(z)-\alpha'(y)} = V_{\alpha'(z)} + V^*_{-\alpha'(y)},$$

by Lemma 1, by the theorem of Riemann-Roch and by the definitions of V and V^* (cf. also Weil [7], Prop. 16), where z is a generic point of C over $k(w,y)$. Since $\alpha(\Gamma)_{w+d}$ is contained in $\theta_d = \theta'$ and since $\alpha'(z) - \alpha'(y) - w$ is a generic point of J over k, it follows that $V_{\alpha'(z)}$ and $\alpha(\Gamma)_{w+d}$ have at least $g-1$ distinct points in common by Weil [7], Th. 20. Thus we have shown that when we put $u = w + d - S(\alpha'(\mathfrak{k}')) - \alpha'(z)$, $V_{-S(\alpha'(\mathfrak{k}'))}$ and $\alpha(\Gamma)_u$ have at least $g-1$ distinct points in common.

Put $D = \alpha'(C)^-$. Then J is the Jacobian variety of D, the injection map of D into J is the canonical mapping of D into J and θ'^- is the set of sums of $g-1$ points on D. Let X' be the subvariety of $J \times D$ with a field of definition k such that when s is a generic point of J over k, $X'(s) = \mathfrak{m} \succ 0$, $\deg(\mathfrak{m}) = g$ and $s = S(\mathfrak{m})$. Then $V_{-S(\alpha'(\mathfrak{k}'))}$ is the set of classes of special D-divisors of degree g. By Lemma 4, $(\alpha(\Gamma)_u \times D) \cdot X'$ is defined. By (i), Lemma 5, we see that, in the expression

$$(\alpha(\Gamma)_u \times D) \cdot X' = T_1 + \mathfrak{a} \times D + \alpha(\Gamma)_u \times \mathfrak{b}_1,$$

we must have $\deg(\mathfrak{a}) \geqq g-1$. Since $(\alpha(\Gamma)_u \times D) \cdot X'$ is a correspondence of type (g,g) on $\alpha(\Gamma)_u \times D$ by the formula (1), $\deg(\mathfrak{a}) = g$ implies $T' = 0$ and $\deg(\mathfrak{b}_1) = g$, which is impossible because of the definition of X' and Weil [7], Th. 19. Hence $\deg(\mathfrak{a}) = g-1$ and T_1 is the graph of a rational mapping of D onto $\alpha(\Gamma)_u$. Since $\dim_k(u) = g-1$, $\alpha(\Gamma)_u$ contains a generic point of J over k. It follows that when $\alpha(x) + u$ is a generic point of $\alpha(\Gamma)_u$ over $k(u)$, then it is a generic point of J over k, and every component of $T_1(\alpha(x)+u)$ has the coefficient 1. Therefore T_1 is the graph of a separable rational mapping f. When that is so, f is a birational mapping by Lemma 2 of the Appendix. Now let us assume that $-\alpha'(y)$ is a generic point of D over $k(u)$; then we have

$$S(f(-\alpha'(y)) + \mathfrak{a}) = -\alpha'(y) + (g-1)u + S(\alpha(\mathfrak{k})) + d + S(\alpha'(\mathfrak{k}')),$$

by (iii), Lemma 5 (Remark: $\theta'^- = \theta^-_{-d} = \theta_{-S(\alpha(\mathfrak{k}))-d}$). Thus we have seen that $\alpha(\Gamma) = D_c = \alpha'(C')^-_c$, where c is a constant rational over $k(u)$. Let h be the birational transformation of Γ to C such that $-\alpha' \cdot h + c = \alpha$; then h is the one we are looking for.

Let h' be a rational transformation of Γ to C such that $\alpha' \cdot h' = \alpha + c'$, where c' is a constant, and let K be a common field of definition for h and h'. Let x be a generic point of Γ over K; then we see that $\alpha'(h(x))+\alpha'(h'(x)) =$ constant, which implies that $l(h(x)+h'(x))>1$ by Weil [7], Th. 19. Since C cannot be a hyperelliptic curve by what we have proved, there exists no such h'. If we have $-\alpha'\cdot h'=\alpha+c'$, then $h(x)+h'(x')=h(x')+h'(x)$ for any two points x and x' on Γ by the same reason as before, which shows that $h(x)=h'(x)$, i.e. $h=h'$. Our theorem is thereby proved.

Appendix.

1. A complete non-singular curve C is called *hyperelliptic*, if it carries a positive divisor $\mathfrak{a}$ of degree 2 such that $l(\mathfrak{a})>1$.

LEMMA 1. *Let C be a complete non-singular curve of genus g, J be its Jacobian variety and α be the canonical mapping of C into J. Let k be a common field of definition for C, J, α and let $\mathfrak{m}$ be a positive C-divisor of degree g such that $S(\alpha(\mathfrak{m}))$ is a generic point of W^* over k. Then $l(\mathfrak{m})=2$; and when C is not a hyperelliptic curve, $\mathfrak{L}(\mathfrak{m})$ is a linear pencil without fixed point.*[2]

Proof. Let F be the rational mapping of the product U of g curves equal to C into J, which is defined by $F(x_1,\cdots,x_g)=\alpha(x_1)+\cdots+\alpha(x_g)$. We have $\dim W^*=g-2$ and $l(\mathfrak{m})>1$ by Weil [7], Prop. 16. If $l(\mathfrak{m})>2$, there must be a generic point $(y_1,\cdots,y_g)$ of U over k such that $F(y_1,\cdots,y_g)$ is $S(\alpha(\mathfrak{m}))$ by Weil [7], Th. 19 and this is impossible. Hence $l(\mathfrak{m})=2$.

By definition of W^*, there is a set $(z_1,\cdots,z_{g-2})$ of $g-2$ independent generic points of C over k such that $\mathfrak{m}\sim\mathfrak{k}-\sum_1^{g-2}(z_i)$, where $\mathfrak{k}$ is a canonical divisor on C. Put $\mathfrak{m}=\sum_1^g(t_i)$, assume that $\mathfrak{L}(\mathfrak{m})$ has a fixed point and let r be the smallest non-negative integer such that $\mathfrak{k}-\sum_1^r(z_i)$ defines a complete linear system with a fixed point z'. Then z' is algebraic over $k(z_1,\cdots,z_r)$, but not algebraic over the field generated by an subset of $(z_1,\cdots,z_r)$ over k. Let z_{g-1} be a generic point of C over $k(z_1,\cdots,z_{g-2})$. Since $l(\mathfrak{k})=g$, with any subset $(z_{i_1},\cdots,z_{i_r})$ of $(z_1,\cdots,z_{g-1})$ we can associate the set of fixed points (z'_i) of the complete linear system $\mathfrak{L}(\mathfrak{k}-(z_{i_1})-\cdots-(z_{i_r}))$; what we have observed shows that if $(z_{i_1},\cdots,z_{i_r})$ and $(z_{j_1},\cdots,z_{j_r})$ are different as sets, then (z'_i) and (z'_j) have no point in common. Let s be the number of points in the set (z'_i), which is independent of i. Then we have

---

[2] The writer owes the proof of the latter half of this lemma to M. Rosenlicht.

$$(g-1)+s\cdot\binom{g-1}{r}\leqq \deg(\mathfrak{f})=2g-2.$$

Therefore we have $r=1$ or $g-2$ and $s=1$. When $r=1$, C is a hyperelliptic curve which we have excluded. Thus we have $r=g-2$ and $s=1$. Let z' be the fixed point of $\mathfrak{L}(\mathfrak{f}-\sum_1^{g-2}(z_i))$, then it is easy to see that z' is rational over $k(z_1,\cdots,z_{g-2})$ (cf. Weil [6], Chap. VIII, Th. 10), which we shall write $z'=f(z_1,\cdots,z_{g-2})$. f is then a symmetric function defined on $C\times\cdots\times C$ ($g-2$ factors) with values in C defined over k and we have

$$\mathfrak{f}\sim\sum_1^{g-1}(z_i)+\sum_j f(z_1,\cdots,z_{j-1},z_{j+1},\cdots,z_{g-1}).$$

By Weil [7], Cor., Th. 7, $\alpha f(z_1,\cdots,g_{g-2})=\sum_i h(z_i)+\text{constant}$, where h is a function defined on C with values in J. Let γ be the linear extension of h, i.e. the endomorphism of J such that $h=\gamma\cdot\alpha+\text{constant}$ (cf. Weil [7], Th. 21). We have $\alpha\cdot f(z_1,\cdots,z_{g-2})=\sum_i\gamma\cdot\alpha(z_i)+\text{constant}$ and

$$S(\alpha(\mathfrak{f}))=\sum_1^{g-1}\alpha(z_i)+(g-2)\cdot\sum_1^{g-1}\gamma\cdot\alpha(z_i)+\text{constant}.$$

Therefore $\alpha(z_i)+(g-2)\cdot\gamma\cdot\alpha(z_i)=c_i$, where c_i is a constant rational over k, since h and γ are defined over k (cf. Weil [7], Cor., Th. 7 and Th. 21). Now let $z_1,\cdots,z_g$ be g independent generic points of C over k. Then we have

$$k(z_1,\cdots,z_g)_s=k(\alpha(z_1)+\cdots+\alpha(z_g))=k((g-2)\cdot\sum\gamma\cdot\alpha(z_i)),$$

which is only possible when $g=3$ (cf. Weil [7], Th. 18). When $g=3$, then we have $r=1$ and our C is a hyperelliptic curve. Our lemma is thereby proved.

Let h be a rational mapping of a variety V onto another variety V'. Let k be a common field of definition for V, V' and h and let x be a generic point of V over k. We say that h is a *separable* (resp. *regular*) *mapping* when $k(x)$ is a separably generated (resp. regular) extension of $k(h(x))$.

LEMMA 2. *Let C and C' be two complete non-singular curves of the same genus and assume that there is a separable rational mapping h from C to C'. Then h is a birational transformation.*

Proof. Let J and J' be the Jacobian varieties of C and C'. We may assume, without loss of generality, that canonical mappings from both curves into their Jacobian varieties are injections. Then the linear extension β of h (cf. Weil [7], Th. 21) is a surjective homomorphism of J to J'. Assume that h^{-1} is not a rational mapping; then the kernel of β does not consist of the neutral element O only. Suppose that the kernel of β consists of a finite set of points $O, a_1, \cdots, a_s$. Let x and y be two generic points of C over a field k of definition for C, C', J, J', h and β. Then $\beta(x) = \beta(y)$ when $h(x) = h(y)$; when that is so, we have $y = x + a_i$ for some i (putting $a_0 = O$). In this case, we have $C = C_{a_i}$ and hence $\theta = \theta_{a_i}$, where θ is the theta-divisor on J corresponding to C. On the other hand, we have $\theta = \theta_t$ if and only if $t = O$ by Weil [7], Cor. 3, Th. 30. Therefore, the kernel of β must form an algebraic subgroup of J of dimension greater than 0. This contradicts our hypothesis that C and C' have the same genus.

Let V be a complete variety, non-singular in co-dimension 1. Let F be a rational mapping of V onto a complete non-singular curve C; then we say that (F, C) defines on V a *pencil of divisors* which consists of $F^{-1}(u)$ with u on C. It is called *linear* when C is a rational curve. When C is a curve of genus g, it is called an *irrational pencil of genus* g. There is a classical theorem, saying that there cannot be an algebraic family of irrational pencils on a curve, which is due to Humbert and Castelnuovo. We shall generalize this theorem to varieties of higher dimension.

LEMMA 3. *Let V be a complete variety, non-singular in co-dimension 1 and let Z be a subvariety of a product $U \times W \times V$. Let k be an algebraically closed common field of definition for V, U, W and Z and assume that, when u is a generic point of U over k, $Z(u)$ is the gfaph of a rational mapping F_u of V onto a complete non-singular curve C_u contained in W. Let v be a generic point of U over $k(u)$, then unless C_u (and consequently C_v) is not a rational curve, (F_u, C_u) and (F_v, C_v) define on V the same irrational pencil.*

Proof. We may assume, without loss of generality, that V is a projective variety. First we shall show that our question can be reduced to the case of curves. Let H be a generic hypersurface over $k(u, v)$. By Weil [6], Chap. V, Prop. 2, Chap. VII, Cor., Th. 10 and Chap. VII, Th. 17, $Z \cdot (U \times W \times V \cdot H)$ is defined, irreducible,

$$(Z \cdot (U \times W \times V \cdot H)) \cdot (u \times W \times V) = (u \times Z(u)) \cdot (U \times W \times V \cdot H),$$

which also can be written as $u \times (W \times V \cdot H) \cdot Z(u)$, is prime rational over the smallest common field of definition for u and H containing k and has the projection C_u on W. Let x be a generic point of V over $k(u, v)$ and put $X = F_u^{-1}(F_u(x))$, $Y = F_v^{-1}(F_v(x))$. Let $\mathfrak{L}_m$ be the linear system of sections of V by hypersurfaces of order m. If m is sufficiently large, $\dim \mathfrak{L}_m \geqq 3$ and the linear subsystem of $\mathfrak{L}_m$, consisting of divisors going through x, induces on any component T of X and Y a linear system of dimension at least 1. Let H_m be a generic hypersurface of order m over $k(u,v,x)$ going through x. Then clearly H_m is a generic hypersurface of order m over $k(u,v)$; moreover, $X\cdot H_m$ and $Y\cdot H_m$ are defined by our choice of $\mathfrak{L}_m$. Since $T\cdot H_m$ is rational over a field of transcendence degree at least 1 over $k(u,v,x)$ by our choice of $\mathfrak{L}_m$, it contains a generic point of T over the algebraic closure of $k(u,v,x)$. By the formula we have shown in the beginning of our proof, if our lemma is true for $V\cdot H_m$, i.e. if $F_u^{-1}(F_u(x))\cdot H_m = F_v^{-1}(F_v(x))\cdot H_m$, then what we have observed in the preceding discussion shows that $F_u^{-1}(F_u(x)) = F_v^{-1}(F_v(x))$. Repeating this process, we see that our lemma is true whenever it is true on a complete non-singular curve Γ in a projective space, since $V\cdot H_m$ is again complete and non-singular (cf. Zariski [11]; Nakai [3]).

Let J be the Jacobian variety of Γ, α be the canonical mapping of Γ into J and K be a common field of definition for J, Γ and α. Let u be a generic point of U over K and t be a generic point of C_u over $K(u)$. Put $F_u^{-1}(t) = \mathfrak{m}$, $S(\alpha(\mathfrak{m})) = s$. Then when x and y are components of $\mathfrak{m}$, we see that s is rational over $K(x)$ (cf. Weil [6], Chap. VI, Th. 12; Weil [7], Th. 1) and that the rational mapping f_u of Γ into J defined by $f_u(x) = s$ is such that $f_u(y) = s$. f_u can be written as $\beta\cdot\alpha + c_u$, where β is an endomorphism of J and c_u is a constant, both defined over $K(u)$ by Weil [7], Th. 21. Since there is no algebraic family of endomorphisms on an abelian variety (Chow [2]), β is actually defined over K. Assume that $\deg(\mathfrak{m}) \geqq 2$ and that the pencil defined on Γ by (F_v, C_v) is different from the pencil defined by (F_u, C_u); in other words, assume that $F_u^{-1}(F_u(x)) \neq F_v^{-1}(F_v(x))$. Then $\mathfrak{m}$ cannot be algebraic over $K(x)$ and hence the field generated over K by components of $\mathfrak{m}$ has at least the dimension 2 over K. Therefore we may assume that $\dim_K(x,y) = 2$. $f_u(x) = f_v(y)$ implies $\beta = 0$ and thus (F_u, C_u) defines on Γ a linear pencil by Weil [7], Th. 19. Consequently, we have

$$Z(u) \sim \mathfrak{a}\times\Gamma + C_u\times\mathfrak{m},$$

where $\deg(\mathfrak{a}) = 1$. Since $Z(u)$ is the graph of a rational mapping of Γ onto C_u, it follows that $t \sim t'$ for any two point on C_u by Weil [6], Chap. VIII, Cor. 1, Th. 4. Thus C_u must be a rational curve. When $\deg(\mathfrak{m}) = 1$, our lemma is trivial and the proof is completed.

2. LEMMA 4. *Let U be a product of n complete non-singular curves Γ_i; let F be a rational mapping of U onto a variety T^n. Let $u = (x_1, \cdots, x_n)$*

be a point on U and denote by $R(i_1,\cdots,i_r)$ the subvariety of U which we get by replacing the i_j-th factor Γ_{i_j} by x_{i_j} for $1 \leqq j \leqq r$ (we assume always that $i_1 < \cdots < i_r$). Assume that F is defined at u, $F(u)$ is simple on T and that the graph of F is transversal to $U \times F(u)$ at $u \times F(u)$ on $U \times T$. Assume also that $F(u)$ is simple on the image $R(i_1,\cdots,i_r)^*$ of $R(i_1,\cdots,i_r)$ by F, for any choice of $(i_1,\cdots,i_r)$. Let V^{n-r} be a subvariety of T, having $F(u)$ as a simple point. Then there is at least one $(i_1,\cdots,i_r)$ such that $R(i_1,\cdots,i_r)^*$ is transversal to V at $F(u)$ on T.

Proof. Let k be a common field of definition for the Γ_i, T, u, F and V. Let W be any subvariety of T having $F(u)$ as a simple point; then there is a subvariety H of T such that H and W are transversal to each other at $F(u)$ on T (cf. for instance Weil [6], Chap. V, Th. 5). Identifying F with its graph and applying Weil [6], Chap. VI, Th. 5 and Th. 6 to $U \times H \cap U \times W \cap F$, we see that a component $\bar{W}$ of $F \cap U \times W$ containing $u \times F(u)$ is uniquely determined, is a proper component of multiplicity 1 on $U \times T$ and has $u \times F(u)$ as a simple point.

F is defined along $R(i_1,\cdots,i_r)$ by Weil [6], Chap. IV, Cor., Th. 15. Then there is the uniquely determined subvariety $R(i_1,\cdots,i_r)'$ on F having the projection $R(i_1,\cdots,i_r)$ on U, which is a proper component of multiplicity 1 in $R(i_1,\cdots,i_r) \times T \cap F$ on $U \times T$ by Weil [6], Chap. VI, Cor., Th. 6 and Th. 8. The image $R(i_1,\cdots,i_r)^*$ of $R(i_1,\cdots,i_r)$ by F is the projection of $R(i_1,\cdots,i_r)'$ on T. When we apply the result just proved in the beginning of this proof to $F \cap U \times V$ and to $F \cap U \times R(i_1,\cdots,i_r)^*$, we see that there are the uniquely determined components $\bar{V}$ and $R(i_1,\cdots,i_r)'$ containing $u \times F(u)$ in them, and that they are proper components of multiplictiy 1 on $U \times T$, having $u \times F(u)$ as simple points. By Weil [6], Chap. VI, Th. 9, we see that

$$i(\bar{V} \cdot (U \times R(i_1,\cdots,i_r)^*), u \times F(u); U \times T)$$
$$= i(\bar{V} \cdot R(i_1,\cdots,i_r)', u \times F(u); F) = i(V' \cdot R(i_1,\cdots,i_r), u; U),$$

where V' is the projection of $\bar{V}$ on U (cf. also Weil [6], Chap. VI, Th. 8). By Weil [6], Chap. VI, Th. 5, we see also that

$$i(V \cdot R(i_1,\cdots,i_r)^*, F(u); T) = i(\bar{V} \cdot (U \times R(i_1,\cdots,i_r)^*), u \times F(u); U \times T),$$

under the assumption that $F(u)$ is a proper component of $V \cap R(i_1,\cdots.i_r)^*$ on T. Passing to representatives, we assume that U and T are affine varieties. Let $S^1{}_i$ be the tangent linear variety to Γ_i at x_i. Then the tangent linear variety to U at u is $S^n = S^1{}_1 \times \cdots \times S^1{}_n$ by Weil [6], Chap. IV, Th. 13.

Since the projection from F to U is biregular at $u \times F(u)$, u is a simple point on V' by Weil [6], Chap. IV, Cor. 1, Th. 17. Then the tangent linear variety S^{n-r} at u to V' is contained in S^n by Weil [6], Chap. IV, Prop. 23. The tangent linear variety to $R(i_1, \cdots, i_r)$ at u is of the form $S(i_1, \cdots, i_r)$ which we get by replacing the i_j-th factor of S^n by x_{i_j} for $1 \leqq j \leqq r$. Now it is clear that at least one of the $S(i_1, \cdots, i_r)$, with $i_1 < \cdots < i_r$, is transversal to S^{n-r} at u on S^n. Let $S(i_1, \cdots, i_r)$ be such; then we have

$$i(V' \cdot R(i_1, \cdots, i_r), u; U) = 1.$$

If $F(u)$ is not a proper component of $V \cap R(i_1, \cdots, i_r)^*$, then $u \times F(u)$ is not a proper component of $V' \cap R(i_1, \cdots, i_r)$ on U and our lemma is thereby proved.

We are going to apply the preceding lemma to the following proposition, which was proved recently by A. Weil (Weil [10], Th. 3) from the consideration of differential forms.

PROPOSITION. *Let J^g be the Jacobian variety of a complete non-singular curve Γ and let α be the canonical mapping of Γ into J. Then a point w' of W^r is simple on W^r if and only if a positive divisor $\mathfrak{m}$ of degree r on Γ such that $S(\alpha(\mathfrak{m})) = w'$ has the property $l(\mathfrak{m}) = 1$.*

Proof. If $l(\mathfrak{m}) = 1$, then w' is simple on W^r by Weil [7], Prop. 18. Therefore, assume that $l(\mathfrak{m}) > 1$. Let U be the product of g curves equal to Γ and let F be the rational mapping of U onto J defined by $F(x_1, \cdots, x_g) = \sum \alpha(x_i)$. Let k be a common field of definition for Γ, J, α, F, w' and let u be a generic point of J over k. Then $w' + u$ is a generic point of J over k. If w' is simple on W^r, $w' + u$ is simple on $W^r{}_u$. Applying the preceding lemma to U, J, F, $W^r{}_u$ and to a generic point $(x_1, \cdots, x_g)$ of U over k such that $\sum \alpha(x_i) = w' + u$, it follows that there is a translation $W^{g-r}{}_t$ of W^{g-r} such that $W^r{}_u$ and $W^{g-r}{}_t$ are transversal to each other at $w' + u$ on J. Hence there is a $W^{g-r}{}_v$ such that it is transversal to W^r at w' on J. There is an $\alpha(\Gamma)_s$ on $W^{g-r}{}_v$ containing w', and when that is so, w' is a simple point of $\alpha(\Gamma)_s$. Take a representative of w' and take representatives of J, $\alpha(\Gamma)_s$, $W^{g-r}{}_v$, W^r on the same affine space. Let us denote by the same letters those representatives we have chosen. Then the tangent linear variety S^1 to $\alpha(\Gamma)_s$ at w' is contained in the tangent linear variety S^{g-r} to $W^{g-r}{}_v$ at w' by Weil [6], Chap. IV, Prop. 23. Since S^{g-r} and the tangent linear variety S^r to W^r at w' are transversal to each other at w' on the tangent linear variety S to J at w', S^1 cannot be contained in S^r. Consequently, $\alpha(\Gamma)_s$ cannot be a subvariety of W^r. Since $\alpha(\Gamma)_s$ contains w', it can be written as $\alpha(\Gamma)_{w'-\alpha(x)}$, where x is a point on Γ. For any point y on Γ, we have $l(\mathfrak{m}-x+y)\geqq 1$ and hence there is a positive divisor $\mathfrak{m}'$ of degree r on Γ such that $\mathfrak{m}'\sim\mathfrak{m}-x+y$. By Weil [7], Th. 19, we have $S(\alpha(\mathfrak{m}'))=S(\alpha(\mathfrak{m}-x+y))$, and this shows that $\alpha(\Gamma)_s$ is contained in W^r, which is a contradiction. Therefore w' cannot be simple on W^r and our proposition is thereby proved.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Andreotti, "Recherches sur les surfaces algébriques irregulières," *Academie Royale de Belgique. Classes des Sciences. Mémoires. Collection in* 8°27, no. 7 (1952).

[2] W. L. Chow, "Abelian varieties over function fields," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 253-257.

[3] Y. Nakai, "Note on the intersection of an algebraic variety with the generic hyperplane," *Memoire of the College of Science, Kyoto University*, Ser. A, vol. 26 (1951), pp. 185-187.

[4] T. Matsusaka, "Polarized varieties, fields of moduli and generalized Kummer varieties of polarized Abelian varieties," *American Journal of Mathematics*, vol. 80 (1958), pp. 45-82.

[5] R. Torelli, "Sulle varietà di Jacobi," *Rendiconti della Reale Accademia dei Lincei*, serie 5ª, vol. 22 (1913), pp. 98-103.

[6] A. Weil, "Foundations of Algebraic Geometry," *American Mathematical Society Colloquium Publications*, vol. 29 (1946).

[7] ———, "Variétés Abéliennes et Courbes Algébriques," *Actualités Scientifiques et Industrielles*, No. 1064 (1948).

[8] ———, "Projective embeddings of Abelian varieties," *Algebraic Geometry and Topology* (A symposium in honor of S. Lefschetz), Princeton Mathematical series, pp. 177-181.

[9] ———, "On the theory of complex multiplication," *Proceedings of the International symposium on Algebraic Number Theory* (1955), pp. 9-22.

[10] ———, "Zum Beweis des Torellischen Satzes," *Nachrichten der Akademie der Wissenschaften in Göttingen.* Mathematisch-Physikalische Klasse, Nr. 2 (1957), pp. 33-53.

[11] O. Zariski, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques Severi," *Annals of Mathematics*, vol. 55 (1952), pp. 552-592.

8

ON A THEOREM OF TORELLI.*

By Aldo Andreotti.

Denote by X an algebraic non-singular curve of genus g in some (complex) projective space $P(\boldsymbol{C})$. Choose on X a base $\gamma_1, \cdots, \gamma_{2g}$ for $H_1(X, Z)$ such that $(I(\gamma_i, \gamma_j)) = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ and a base $\omega_1, \cdots, \omega_g$ for $H^0(X, \Omega^1)$ (differentials of the first kind). Denote by $\omega(X)$ the matrix of the periods $\omega = (\int_{\gamma_i} \omega_j)$.

The classical form of Torelli's theorem is as follows: *two curves X, X' of the same genus g are birationally equivalent if (and only if) the bases $\{\gamma_i\}$ $\{\omega_j\}$ may be so chosen that $\omega(X) = \omega(X')$.*[1]

In a recent paper, A. Weil [9(c)] has given an abstract form of this statement which is as follows: *two curves X, X' are birationally equivalent if (and only if) there exists an isomorphism of the Jacobian variety $J(X)$ of X onto the Jacobian variety $J(X')$ of X' which carries the canonical polarization of $J(X)$ into the canonical polarization of $J(X')$.*

Now it is possible to give to Torelli's theorem a simpler and (apparently) more general form from which the classical as well as the abstract formulation can be easily deduced.

The statement is as follows: *The necessary and sufficient condition for two curves X, X' of the same genus g to be birationally equivalent is that their symmetric products $(X)^{(g-1)}$, $(X')^{(g-1)}$ be birationally equivalent.*

The previously given forms of Torelli's theorem follow at once from the remark that the symmetric product $(X)^{(g-1)}$ is birationally equivalent to the canonical Θ-divisor on $J(X)$,[2] and the fact, proved by A. Weil,[3] that the canonical polarization determines uniquely the Θ-divisor.

---

* Received February 24, 1958.

[1] Once the base $\{\gamma_i\}$ is chosen, we may normalize the base $\{\omega_j\}$ in such a way that $\omega(X)$ is of the form (I, A). Torelli's theorem may then be expressed by saying that *the necessary and sufficient condition for two curves X, X' to be birationally equivalent is that the matrices $\omega(X) = (I, A)$, $\omega(X') = (I, A')$ be congruent modulo a transformation of Siegel's modular group.*

[2] See A. Weil [9, (b)], p. 71 (Prop. 15).

[3] A. Weil [9, (c)], Theorem 1. In the classical formulation, from $\omega(X) = \omega(X')$

the natural projection of y on Y/Γ. If the point y has as many transforms as there are elements in Γ, then y and $p(y)$ are both simple or singular.

Denote by $I(Y) = k[x_1, \cdots, x_n]$ the coordinate ring of Y and let $j_1, \cdots, j_s$ be a set of generators for the subring of Γ-invariants; the ring $I(Y/\Gamma)$ of coordinates on Y/Γ may be assumed to be the ring $k[j_1, \cdots, j_s]$.

Since the j's are polynomials in the x's, we have relations (α) $dj_h = \sum (\partial j_h/\partial x_i)_y \, dx_i$. Conversely, since k is infinite, we may suppose that the transforms of y have all the i-th coordinates x_i two by two distinct $1 \leqq i \leqq n$. The x_i's are integers over $k[j_1, \cdots, j_s]$ and hence satisfy equations of the type $x_i^q + a_1(j) x_i^{q-1} + \cdots + a_q(j) \equiv f_i(x_i, j) = 0$. By the above hypothesis, we must have $(\partial f_i/\partial x_i)_y \neq 0$; therefore the relations (α) may be solved with the expressions (β) $dx_i = -(\partial f_i/\partial x_i)_y^{-1} \sum (\partial f_i/\partial j_h)_{p(y)} dj_h$. Now $\dim Y = \dim Y/\Gamma$, and this enables us to conclude that if P describes the ideal $\mathfrak{p}(Y)$ of the polynomials in $k[X_1, \cdots, X_n]$ vanishing on Y, and Q describes the ideal $\mathfrak{p}(Y/\Gamma)$ of the polynomials in $k[J_1, \cdots, J_s]$ vanishing on Y/Γ, there are as many solutions linearly independent for the system $\sum (\partial P/\partial X_i)_y \, dX_i = 0$ as for the system $\sum (\partial Q/\partial J_h)_{p(y)} dJ_h = 0$. This proves the lemma.

If we apply the lemma to the case in which Y is an open subset of $(X)^q$ invariant under Γ, we easily infer the following:

PROPOSITION 1. *If X is a projective variety of dimension d, irreducible and non-singular, the symmetric product $(X)^{(\Gamma)}$ has a singular locus of dimension $\leqq (q-1)d$.*

c) Let us suppose now that X is an irreducible algebraic projective variety of dimension 1 (i.e., a curve) and consider the usual symmetric product $(X)^{(q)}$. We have the following useful

PROPOSITION 2. *The symmetric product $(X)^{(q)}$ of an algebraic non-singular curve X is non-singular.*

Let $(A_1) + \cdots + (A_q) = z$ be a point of $(X)^{(q)}$ and suppose we have $A_1 + \cdots + A_q = n_1 P_1 + \cdots + n_r P_r$ with $P_i \neq P_j$ and $\sum n_i = q$. The point z may be supposed in an affine open set of type $(U)^{(q)}$, U being an affine open set on X containing $P_1, \cdots, P_r$. Moreover, we may suppose there is a regular function t on U such that i) $t - (t)_{P_i}$ is a uniformizing parameter on X at P_i for $1 \leqq i \leqq r$, ii) $(t)_{P_i} \neq (t)_{P_j}$ if $i \neq j$. Denote by t_s the regular function induced on $(U)^q$ by the projection on the s-th factor by the function t on U. Put $\phi_1 = t_1 + \cdots + t_q, \cdots, \phi_q = t_1 \cdots t_q$; these are rational regular functions on $(U)^q$ and invariant under G_q, hence rational functions on $(X)^{(q)}$ regular at z. Let R be a rational function on $(X)^{(q)}$ regular at z. If we lift R to $(X)^q$, R will become a rational function, invariant under $\boldsymbol{G}_q$, and regular at $A_1 \times \cdots \times A_q$ (and hence also at the $r!$ transforms of $A_1 \times \cdots \times A_q$). Now the parameters $t_1 - (t_1)_{A_1}, \cdots, t_q - (t_q)_{A_q}$ are uniformizing parameters at $A_1 \times \cdots \times A_q$. Hence we may find for each integer m a polynomial of degree m, $P_m(t_1 - (t_1)_{A_1}, \cdots, t_q - (t_q)_{A_q})$ such that $R - P_m \in \mathcal{O}_{A_1 \times \cdots \times A_q}(t_1 - (t_1)_{A_1}, \cdots, t_q - (t_q)_{A_q})^{m+1}$ ($\mathcal{O}_{A_1 \times \cdots \times A_q} =$ local ring at $A_1 \times \cdots \times A_q$). Since R is $\boldsymbol{G}_q$-invariant, we deduce that

$$P_m(\cdots, t_i - (t_i)_{A_i}, \cdots, t_j - (t_j)_{A_j}, \cdots) \\ = P_m(\cdots, t_j - (t_j)_{A_j}, \cdots, t_i - (t_i)_{A_i}, \cdots).$$

This property shows that P_m may be expressed as a polynomial in $\phi_1 - (\phi_1)_z, \cdots, \phi_q - (\phi_q)_z$. This last statement is an immediate consequence of our proposition for the case $X = k$. This proves the proposition in general.

2. Holomorphic forms on symmetric products. a) Let X be an abstract variety, U an open subset of X. An expression of the type $\omega^{(k)} = \sum X_{i_1 \cdots i_k} dY_{i_1} \cdots dY_{i_k}$, where the X's and Y's are rational functions on U, will be said to be a meromorphic k-form on U. With the obvious restriction of an open set U on an open subset $V \subset U$, we get the definition of the sheaf $\mathfrak{M}^{(k)}$ of meromorphic k-forms on X. If X is an irreducible variety of dimension d and $k(X)$ is the field of rational functions on X, the space $H^0(X, \mathfrak{M}^{(k)})$ is a vector space over $k(X)$ of dimension $\binom{d}{k}$. Any system $x_1, \cdots, x_d$ of elements of $k(X)$ which give a separating transcendency base for $k(X)$ generates, by the differentials $dx_1, \cdots, dx_d$, the whole space of meromorphic k-forms.

b) Let P be a point of X. The form $\omega^{(k)}$ will be said to be holomorphic at P if it has an expression in which the X's and Y's are regular at P. In particular, if P is a simple point and $t_1, \cdots, t_d$ are uniformizing parameters at P, a holomorphic form $\omega^{(k)}$ at P may be written in a *unique* way as $\sum \phi_{i_1 \cdots i_k}(t_1, \cdots, t_d) dt_{i_1} \wedge \cdots \wedge dt_{i_k}$, where the $\phi_{i_1 \cdots i_k}$ are regular at P and expressible as formal power series in the t's. A k-form holomorphic at each point of the open set U will be said to be holomorphic in U. The sheaf of holomorphic k-forms on X will be denoted by $\Omega^{(k)}$. As well as the holomorphic k-forms on X, i.e. the elements of the space $H^0(X, \Omega^{(k)})$, one may consider the holomorphic tensor forms on X, i.e. the elements of spaces of the type $H^0(X, \Omega^{(k_1)} \otimes \cdots \otimes \Omega^{(k_r)})$, the tensor product being taken over the sheaf of local rings.

c) We want to compute the dimension of some of the above mentioned vector spaces for the case in which X is the symmetric product of a projective curve. The easiest way to do it is to give first the computation for the cartesian product and then deduce from it the calculus of the vector spaces being considered.

For a cartesian product, the computation is a straightforward conseqence of the Künneth formula that will be recalled here.

LEMMA.[6] *Let X, Y be two non-singular irreducible abstract varieties. There exist coverings U_i of X, V_j of Y with affine open sets such that on the covering W_{ij} of $X \times Y$, where $W_{ij} = U_i \times V_j$, we have*

$$H^0(W_{ij}; \Omega^{(k_1)} \otimes \cdots \otimes \Omega^{(k_r)})$$
$$\approx \sum_{\substack{p_h+q_h=k_h \\ 1 \leqq h \leqq r}} H^0(U_i; \Omega^{(p_1)} \otimes \cdots \otimes \Omega^{(p_r)}) \otimes H^0(V_j; \Omega^{(q_1)} \otimes \cdots \otimes \Omega^{(q_r)}).$$

The lemma being of a local nature, we may assume X, Y to be affine varieties. Let P be a point in X, and denote by $X_1, \cdots, X_d$, $d = \dim X$, d rational functions on X, regular at P and such that the functions $t_i = X_i - X_i(P)$ are uniformizing parameters at P. Now there exists an open neighborhood U_P of P such that for any point $Q \in U_P$, the functions $X_i - X_i(Q)$ are uniformizing parameters at Q. Hence we have a covering of X, $\{U_P\}_{P \in X}$. Similarly, we define the covering $\{V_Q\}_{Q \in Y}$ of Y. Refining, if necessary, these coverings, we may suppose that the U_i (V_j) are affine varieties so that we are reduced to proving the lemma for two affine varieties X, Y which may be covered by a global system of uniformizing parameters: X_i, $1 \leqq i \leqq \dim X$; Y_j, $1 \leqq j \leqq \dim Y$. At this stage, the proof becomes evident since the ring of coordinates on $X \times Y$ is the tensor product of the rings of coordinates on X and Y.

The lemma shows that the cohomology of $X \times Y$ with coefficients in the sheaf $\Omega^{(k_1)} \otimes \cdots \otimes \Omega^{(k_r)}$ may be computed as the cohomology of the complex which appears on the right hand side of the above formula. This last is a sum of cartesian products of complexes defined for the spaces X, Y respectively. Applying now the Eilenberg-Zilber theorem [2] we get the *Künneth formula*:[7]

---

[6] For a similar case, see J. P. Serre [7, (b)], Ch. VII, n. 5.

[7] We get an analogous formula if we consider instead of the sheaf of cotangent vectors and its exterior algebra, the sheaf of tangent vectors.

$$H^q(X\times Y;\Omega^{(k_1)}\otimes\cdots\otimes\Omega^{(k_r)})$$
$$=\sum_{\substack{p_h+q_h=k_h\\ 1\leqq h\leqq r}}\sum_{a+b=q} H^a(X;\Omega^{(p_1)}\otimes\cdots\otimes\Omega^{(p_r)})\otimes H^b(Y;\Omega^{(q_1)}\otimes\cdots\otimes\Omega^{(q_r)}).$$

3. a) We will apply the Künneth formula to the simple case in which $k_1=k_2=\cdots=k_r=\dim X+\dim Y$ to get the plurigenera of the product $X\times Y$. In this case, let us put $\mathcal{H}_r{}^*(X)=\sum_{q\geqq 0} H^q(X,\underbrace{\Omega^{(d)}\otimes\cdots\otimes\Omega^{(d)}}_{r\text{ times}})$, where $d=\dim X$, and similarly define the groups $\mathcal{H}_r{}^*(Y)$ and $\mathcal{H}_r{}^*(X\times Y)$. Then the Künneth formula reduces to

$$\mathcal{H}_r{}^*(X\times Y)=\mathcal{H}_r{}^*(X)\otimes\mathcal{H}_r{}^*(Y).$$

In particular, if we denote by $P_r(X)$ the $\dim_k H^0(X,\underbrace{\Omega^{(d)}\otimes\cdots\otimes\Omega^{(d)}}_{r\text{ times}})$ (r-genus of X), we get the formula $P_r(X\times Y)=P_r(X)P_r(Y)$.

Suppose that X is an algebraic projective irreducible curve. For the cartesian product $(X)^q$, we get the following formulae:

$$P_1((X)^q)=g^n;P_r((X^q)=(2r-1)^q(g-1)^q, r\geqq 2,$$

where g is the genus of the curve X.

b) Consider now the symmetric product $(X)^{(q)}$ of the curve X. Taking into consideration the regular map $\pi\colon (X)^q\to(X)^{(q)}$, any holomorphic form on $(X)^{(q)}$ may be lifted to $(X)^q$ and there it will be an element of the space of holomorphic forms of that type invariant under the symmetric group G_q.

In particular, for the plurigenera, we will have the inequality

$$P_r((X)^{(q)})\leqq\dim\{H^0((X)^q,\underbrace{\Omega^{(q)}\otimes\cdots\otimes\Omega^{(q)}}_{r\text{ times}})\}^{G_q},$$

where the symbol $\{\ \}^{G_q}$ indicates the subspace of fixed elements under G_q of the space in the brackets.

c) For the case $r=1$ (geometric genus), we have the following:

PROPOSITION 3. i) *Denote by* $\omega_\alpha(x)$, $1\leqq\alpha\leqq g$, *a base for* $H^0(X,\Omega^1)$. *Any q-form* $\Omega\in H^0((X)^q,\Omega^{(q)})$ *is of type*

$$\Omega=\sum c_{\alpha_1\cdots\alpha_q}\omega_{\alpha_1}(x_1)\wedge\cdots\wedge\omega_{\alpha_q}(x_q),$$

where $1\leqq\alpha_i\leqq g$ *and* $c_{\alpha_1\cdots\alpha_q}\in k$.

ii) *If the characteristic p of the field k is not 2, then any q-form $\Omega \in \{H^0((X^q, \Omega^{(q)})\}^{G_q}$ is of type*

$$\Omega = \sum_{\alpha_1 < \cdots < \alpha_q} c_{\alpha_1 \cdots \alpha_q} \operatorname{Det.} \begin{pmatrix} \omega_{\alpha_1}(x_1), \cdots, \omega_{\alpha_q}(x_1) \\ \cdots\cdots\cdots \\ \omega_{\alpha_1}(x_q), \cdots, \omega_{\alpha_q}(x_q) \end{pmatrix}.$$

If $p = 2$, then a set of independent generators for the G_q-invariant q-forms is given by the expressions $\sum \sigma_i(\omega_{\alpha_1}(x_1) \wedge \cdots \wedge \omega_{\alpha_q}(x_q))$, where σ_i runs over a system of representatives of $G_q/h_{(\alpha_1 \cdots \alpha_q)}$, $h_{(\alpha_1 \cdots \alpha_q)}$ being the subgroup of G_q which leaves fixed the permutation $(\alpha_1 \cdots \alpha_q)$.

iii) *For any value of the characteristic p, if $\pi\colon (X)^q \to (X)^{(q)}$ is the natural map, then any form $\Omega \in \pi^* H^0((X)^{(q)}, \Omega^{(q)})$ is of type:*

$$\Omega = \sum_{\alpha_1 < \cdots < \alpha_q} c_{\alpha_1 \cdots \alpha_q} \operatorname{Det.} \begin{pmatrix} \omega_{\alpha_1}(x_1), \cdots, \omega_{\alpha_q}(x_1) \\ \cdots\cdots\cdots \\ \omega_{\alpha_1}(x_q), \cdots, \omega_{\alpha_q}(x_q) \end{pmatrix}.$$

The points i) and ii) are obvious consequences of the Künneth formula and of a self-evident computation. Only point iii) deserves a little attention.

For that purpose, cover $(X)^{(q)}$ by affine open sets of the form $(U)^{(q)}$, where we take as uniformizing parameters the symmetric functions $\phi_1 = t_1 + \cdots + t_q, \cdots, \phi_q = t_1 \cdots t_q$ (the function $t_i - (t_i)_P$ being a uniformizing parameter at P on the i-th factor U of $(U)^q$) [8]. We get the expression: $d\phi_1 \wedge \cdots \wedge d\phi_q = \prod_{i<j} (t_i - t_j)\, dt_1 \wedge \cdots \wedge dt_q$. Now obviously

$$\pi^* H^0((X)^{(q)}, \Omega^q) \subset \{H^0((X)^q, \Omega^{(q)})\}^{G_q},$$

and the necessary and sufficient condition for a G_q-invariant q-form Ω of $(X)^q$ to be the image of a form on $(X)^{(q)}$ is that on any open set $(U)^q$, $\Omega(\prod(t_i - t_j))^{-1}$ be holomorphic there. Now the only invariant elements which satisfy this condition are the forms of the type given as one verifies.

4. A digression on the invariance of holomorphic forms.

The importance of holomorphic forms on an algebraic variety lies in the fact that these are birational invariants. Precisely, we have the

THEOREM. *Let X, Y be two algebraic varieties, of the same dimensions, both irreducible and* non-singular. *Let $\phi\colon X \to Y$ be a birational map of X into Y. Then there is a natural*[9] *isomorphism*

---

[8] Cf. Proposition 2.

[9] The isomorphism is the one induced by the isomorphism between the spaces of global meromorphic forms.

$$\phi^*: H^0(Y,\Omega^*) \to H^0(X,\Omega^*) \quad (\Omega^* = \Omega^{(p_1)} \otimes \cdots \otimes \Omega^{(p_r)}).$$

This theorem has been proved for the abstract case by Koizumi [5]. Another proof has been announced by Cartier [1]. We give here a proof close to the classical one.[10]

LEMMA 1. *The mapping* ϕ^{-1} *is regular on* Y *outside an algebraic subset of dimension* $\leqq d-2$.

Since X is complete, $\phi(X)$ (i.e. the projection on Y of the closed graph of ϕ on $X \times Y$) is closed in Y; since ϕ is birational, $\phi(X)$ contains an open subset of Y; since Y is irreducible $\phi(X) = Y$. Hence it is enough to prove the lemma for the case in which Y is an affine variety, X an algebraic variety and $\phi: X \to Y$ a regular map of X onto Y: $\phi(X) = Y$.

Let $\{U_i\}$ be an open covering of X of affine varieties U_i; denote by x_{U_i} the coordinates on U_i and y the coordinates on Y. The birational map is then given by equations $y = P_{U_i}(x_{U_i})$, $x_{U_i} = Q_{U_i}(y)$, where the P_{U_i} are polynomials in the x_{U_i}'s and the Q_{U_i} are rational functions of y. Let $x_0 \in U_i$ be a point of X; if in $y_0 = \phi(x_0)$, each Q_{U_i} or its inverse is regular, then ϕ^{-1} is regular at y_0. In fact, we have the identities $Q_{U_i,\alpha}(P_{U_i}(x_{U_i})) = x_{U_i,\alpha}$ as rational functions in $k(U_i)$; now if the Q_{U_i}'s are regular at y_0, ϕ^{-1} is obviously regular there. If, say, $Q_{U_i,\alpha}$ is not regular at y_0, but $Q_{U_i,\alpha}{}^{-1} = R$ is regular at y_0, we must have $R(y_0) = 0$. Hence in the identity $x_{U_i,\alpha} R(P_{U_i}(x_{U_i})) = 1$, specializing $x_{U_i} \to x_0$, we get a contradiction. Therefore the above assertion is proved.

The lemma will be proved if we prove

LEMMA 2. *Let* V *be an affine irreducible variety of dimension* d *whose singular set is of dimension* $\leqq d-2$, *and let* R *be a rational non-zero function on* V. *The locus where* R *and* R^{-1} *are not regular is an algebraic subvariety of dimension* $\leqq d-2$.

If R is regular at a point, it is regular in an open neighborhood of that point. Hence the set where R is not regular is a closed set F_R; $F_R \cap F_{R^{-1}} = W$ is also closed, hence the locus W is algebraic. If $\dim W = d-1$, one may find a point $P \in V$ such that

i) P is simple on V, ii) P belongs to an irreducible component of dimension $d-1$ of W, say W_1.

At P, the local ring $\mathcal{O}_P$ on V is a unique factorization domain (since this is so for its completion). Hence the variety W_1 is represented in $\mathfrak{O}_P$ by a prime ideal $\mathfrak{p}_1$ of dimension $d-1$, and thus is principal: $\mathfrak{p}_1 = \mathfrak{O}_P\pi$. We may suppose π represented by a polynomial.

---

[10] See [9, (a)], Ch. V, Theorems 8 and 13.

Now let R be of the form p/q, where p, q are polynomials. In $\mathfrak{O}_P$, $p = \pi^\alpha p_1$, $q = \pi^\beta q_1$ with p_1, q_1 not in $\mathfrak{p}_1$. We have $R = \pi^{\alpha-\beta} p_1/q_1$. Suppose, for instance, $\alpha \geqq \beta$; then R is regular where p_1, q_1 are regular and $q_1 \neq 0$. Now there is at least one point on W_1 where p_1, q_1 are regular and $q_1 \neq 0$. In fact, p_1, q_1 are regular at P, hence in an open set on W_1. If $q_1 = 0$ contains W_1, by Hilbert's nullstellensatz, we have $q_1 \in \mathfrak{p}_1$. This is a contradiction.

To get the theorem, we have only to make use of a covering of X, Y of the type used in the lemma of n. 2 and combine lemma 1 with the following proposition, which is an abstract form of a theorem of Hartogs.

PROPOSITION 4. *Let V be an irreducible affine* normal *variety of dimension d; let W be a subvariety of V of dimension $\leqq d-2$ and let t be a rational regular function defined on $V-W$. The function t may be extended in a unique way to all V by a rational regular function.*

Denote by $\mathfrak{p}(W)$ the ideal defining the variety W in the ring $I(V)$ of coordinates on V. Let $a \in \mathfrak{p}(W)$, $a \neq 0$, and consider the ideal $I(V)a$. Since V is normal, this ideal $I(V)a$ is pure of dimension $d-1$, i.e. we have a primary decomposition $I(V)a = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_h$ with the $\mathfrak{q}_i$'s primary and associated to prime ideals $\mathfrak{p}_i$ of dimension $d-1$. Now we can find an element $b \in \mathfrak{p}(W)$ such that a and b are relatively prime (i.e. if $b \mid ac$, then $b \mid c$). In fact, denote by α_i a zero of $\mathfrak{p}_i$ which is not a zero of $\mathfrak{p}$ (W) and by l the maximum degree of the polynomials of a base of $\mathfrak{p}(W)$ as an ideal in $k[x]$. Since W is the locus of common zeros for the polynomials of $\mathfrak{p}(W)$ of degree $\leqq l$, the polynomials of $\mathfrak{p}(W)$ of degree $\leqq l$ vanishing on α_i form a proper subspace of the vector space of polynomials of $\mathfrak{p}(W)$ of degree $\leqq l$. Hence there exists a polynomial b (of degree $\leqq l$) in $\mathfrak{p}(W)$ such that $b(\alpha_i) \neq 0$ for $1 \leqq i \leqq h$, i.e. $b \notin \mathfrak{p}_i$, and this implies that b is prime to a.

Now $I(V)(a,b) \subset \mathfrak{p}(W)$ and has dimension $\leqq d-2$. We may suppose, without loss of generality, that W is the locus $a = b = 0$.

By hypothesis, t is an element of $\Gamma(V-W, \mathfrak{O} \mid V-W)$, where $\mathfrak{O}$ is the sheaf of local rings on V, hence for each point $P \in V-W$ we have an expression $t = r_P/s_P$ with r_P, s_P polynomials of $k[x]$ and $s_P(P) \neq 0$.

Since V is irreducible, the open sets $s_P \neq 0$, $s_Q \neq 0$ intersect in an open set on which $r_P s_Q = r_Q s_P$ (outside W), hence this equality holds as an identity in $I(V)$. Moreover, the functions s_P cannot have common zeros outside W.

Therefore a and b vanish on the zeros of the ideal generated by s_P, $P \in V - W$. By Hilbert's nullstellensatz, we can find a suitable integer ρ such that the following relations are satisfied: $a^\rho = \sum a_P s_P$, $b^\rho = \sum b_P s_P$ with the a_P's, b_P's almost all zeros.

Consider the two rational functions

$$t_a = (1/a^\rho) \sum a_P r_P, \qquad t_b = (1/b^\rho) \sum b_P r_P$$

on the open set $a \neq 0$. We have $t - t_a = 0$; similarly, on $b \neq 0$, we have $t = t_b$. Therefore on $a \neq 0$, $b \neq 0$, we have $t_a = t_b$ and hence the identity in $I(V)$: $a^\rho \sum b_P r_P = b^\rho \sum a_P r_P$. Since b is prime to a, we get $b^\rho \mid \sum b_P r_P$, i.e. $\sum b_P r_P = b^\rho \theta$ with $\theta \in I(V)$. Hence $t = \theta$, so t can be extended by θ to all V. The extension is unique since two such functions coincide on an open set of V.

Section 2. Canonical mappings of symmetric products.

5. **Canonical mappings.** a) Denote by $\omega_{\alpha_1 \cdots \alpha_q}$ the base for the holomorphic q-forms on $(X)^{(q)}$ described in Proposition 3. Assuming the $\omega_{\alpha_1 \cdots \alpha_q}$ as homogeneous coordinates on a projective space $P_{d(q)}(k)$, we are led to consider the mapping $\phi^{(q)}$ given by $x \rightarrow \omega_{\alpha_1 \cdots \alpha_q}(x)$ of $X^{(q)}$ into $P_{d(q)}(k)$.[11]

Since $d(q) = \binom{g}{q} - 1$, those mappings have interest only if $1 \leqq q \leqq g - 1$. The cases $q = 1$, $q = g - 1$ will have particular interest.

b) *The case* $q = 1$. A curve X of genus $g > 1$ is said to be hyperelliptic if it contains a linear series $g^1{}_2$ of degree 2 and (projective) dimension 1. This is equivalent to saying that the field $k(X)$ is a quadratic extension of a field of genus zero. We have the following:

PROPOSITION 5. *Suppose that X is of genus $g > 1$. The image $C = \phi(X)$ of X by the canonical map is non-singular; if X is not hyperelliptic, then $\phi\colon X \rightarrow C$ is biregular; if X is hyperelliptic, then the canonical map may be factored into the map: $X \rightarrow P_1(k)$ given by the subfield of genus 0 of $k(X)$ and the biregular map of $P_1(k)$ onto a rational normal curve*[12] *of $P_{g-1}(k)$.*

If two places A, B of X have the same center on C, the residual series, with respect to the canonical series, of $A + B$ will be of degree $2g - 4$ and dimension $g-2$. By the theorem of Riemann-Roch (in the form of the reciprocity theorem), the dimension x of $|A+B|$ will be given by

---

[11] These are rational maps, not necessarily regular.

[12] I. e. a projective transform of the curve with the general point $(1, \lambda, \lambda^2, \cdots, \lambda^{g-1})$.

$$(2g-4)-2=2(g-2)-x.$$

Hence $x=1$ and X is hyperelliptic. This shows that the canonical map ϕ is one-to-one if X is not hyperelliptic..

Assume now that X is not hyperelliptic, and let us suppose that ϕ is not biregular at a point $A \in X$. Denote by $\mathcal{O}_A$, $\mathcal{O}_{\phi(A)}$ the local rings of A, $\phi(A)$ respectively on X, C. The map ϕ induces a monomorphism $\phi^*\colon \mathcal{O}_{\phi(A)} \rightarrow \mathcal{O}_A$ since ϕ is one-to-one. Moreover $\phi^*\mathcal{O}_{\phi(A)} \subsetneqq \mathcal{O}_A$ since ϕ is not biregular at A.

Denote by y_i non-homogeneous coordinates on C, $\phi(A)$ being supposed at the origin. We must have $v_A(\phi^* y_i) \geqq 2$, hence, for any hyperplane $\sum a_i y_i = 0$ containing $\phi(A)$, we get $v_A(\phi^* \sum a_i y_i) \geqq 2$. This shows again that the linear series $|2A|$ will have dimension 1, contrary to the fact that X is not hyperelliptic.

Hence if X is not hyperelliptic, it follows that $\phi\colon X \rightarrow C$ is a biregular map, and C is therefore non-singular.

If X is hyperelliptic, we have only to recall that the canonical series is compounded with the $g^1{}_2$ and that therefore it is the image on X, by ϕ^{-1}, of the series of all divisors of degree $g-1$ on $P_1(k)$.

c) *The general case.* If x is a general point on X, $\omega_1(x),\cdots,\omega_g(x)$ are the homogeneous coordinates of a general point on the canonical model C of X. If $x_1,\cdots,x_q$ are q independent general points on X, then

$$\omega_{a_1\cdots a_q} = \text{Det.}\begin{pmatrix} \omega_{a_1}(x_1),\cdots,\omega_{a_q}(x_1) \\ \cdots\cdots\cdots\cdots \\ \omega_{a_1}(x_q),\cdots,\omega_{a_q}(x_q) \end{pmatrix}$$

are the Plucker's coordinates of the projective space $P_{q-1}(k)$ spanned by the q points $(\omega_1(x_i),\cdots,\omega_g(x_i))$, $1 \leqq i \leqq q$. (These are linearly independent since C belongs to $P_{g-1}(k)$.) We deduce the following *geometric construction of the canonical map*:

The canonical model $C^{(q)}$ of the symmetric product $(X)^{(q)}$, $1 \leqq q \leqq g-1$, ($g=$ genus of the curve X) has for general point the point of the Grassmann manifold $G_{q-1,g-q}$ (of the spaces P_{q-1} in P_{g-1}) which is the image of the space P spanned by q general points of the canonical curve C.

In particular, for $q=g-1$, the canonical model $C^{(g-1)}$of $(X)^{(g-1)}$ is the projective space $P_{g-1}{}^*(k)$ dual to the space $P_{g-1}(k)$ of the canonical curve C.

d) The canonical maps $\phi^{(q)}$ are rational maps but not necessarily regular maps (if $q > 1$).

PROPOSITION 6. *Let* $(A_1) + \cdots + (A_q)$ *be the point of* $(X)^{(q)}$ *corresponding to the divisor* $A_1 + \cdots + A_q$ *on* X. *Then* $\dim | A_1 + \cdots + A_q | \geqq 1$ *if and only if for any holomorphic q-form* Ω *on* $(X)^{(q)}$, *we have* $\Omega((A_1) + \cdots + (A_q)) = 0$ (*i.e. the point* $(A_1) + \cdots + (A_q)$ *is a base point of the canonical system*).

Let $A_1 + \cdots + A_q = n_1P_1 + \cdots + n_rP_r$ with $P_i \neq P_j$ and $\sum n_i = q$. Let ω_α, $1 \leqq \alpha \leqq g$, be a base for holomorphic 1-forms on X. Choose a local parameter t_P at the point P on X and write

$$\omega_\alpha = \{\phi_\alpha(P) + \phi_\alpha'(P)t_P + \phi_\alpha''(P)t_P^2 + \cdots\}dt_P.$$

The condition $\dim | A_1 + \cdots + A_q | > 1$ means that the specialty index $i(A_1 + \cdots + A_q) > g - q$. Now $i(A_1 + \cdots + A_q) = s$ means:

$$\operatorname{rank}(\phi(P_1), \cdots, \phi^{(n_1-1)}(P_1); \cdots; \phi(P_r), \cdots, \phi^{(n_r-1)}(P_r)) = g - s,$$

where the symbol $\phi^{(s)}(P_i)$ stands for the column vector $\phi_\alpha^{(s)}(P_i)$.

Using the notation of Proposition 2, if $r = 1$, for the form

$$\Omega_{\alpha_1 \cdots \alpha_q} = \{(\sum \omega_{\alpha_1}(Q_i)) \wedge \cdots \wedge (\sum \omega_{\alpha_q}(Q_i))\}\{\Pi((t)_{Q_i} - (t)_{Q_j})\}^{-1},$$

we get the expression at P_1:[13]

$$\Omega_{\alpha_1 \cdots \alpha_q}(P_1) = \text{Det.}\begin{pmatrix} \phi_{\alpha_1}(P_1), \cdots, \phi_{\alpha_1}^{(n_1-1)}(P_1) \\ \cdots\cdots\cdots \\ \phi_{\alpha_q}(P_1), \cdots, \phi_{\alpha_q}^{(n_1-1)}(P_1) \end{pmatrix} \cdot d\phi_1 \wedge \cdots \wedge d\phi_{n_1} \qquad (n_1 = q).$$

In the general case, we get therefore

$$\Omega_{\alpha_1 \cdots \alpha_q}(n_1(P_1) + \cdots + n_r(P_r)) \\ = \{\prod_{i<j}((t)_{P_i} - (t)_{P_j})\}^{-1} \sum \Omega_{a_1 \cdots a_{n_1}}(P_1) \wedge \cdots \wedge \Omega_{c_1 \cdots c_{n_r}}(P_r),$$

where $(a_1, \cdots, c_{n_r})$ is any permutation of $(\alpha_1, \cdots, \alpha_q)$ and in the product, each factor has to be taken the correct number of times. The differentials on the right side at $(A_1) + \cdots + (A_q)$ have for jacobian with respect to $d\phi_1, \cdots, d\phi_q$ the product which appears in the formula. It follows that the

---

[13] From the obvious identity:

$$\begin{pmatrix} \phi_{a_1}(P) \cdots & \\ \cdots & \\ \cdots \phi_{a_q}^{(q-1)}(P) \end{pmatrix}\begin{pmatrix} 1 & \cdots & 1 \\ \theta_1 & \cdots & \theta_q \\ \theta_1^{q-1} & \cdots & \theta_q^{q-1} \end{pmatrix} = \begin{pmatrix} \sum \phi_{a_1}^{(s)}\theta_1^s, \cdots & \\ & \cdots, \sum \phi_{a_q}^{(s)}\theta_q^s \end{pmatrix}$$

by taking the determinants and putting $\theta_i = t_i - (t_i)_P$.

condition $\Omega((A_1)+\cdots+(A_q))=0$ means that all minor determinants of order q of the above matrix are zero. q. e. d.

COROLLARY. *The map* $\phi^{(q)}$ *is regular at* $(A_1)+\cdots+(A_q)$ *if*

$$\dim. |A_1+\cdots+A_q|=0.^{14}$$

We finally remark that the canonical models $C^{(q)}=\phi^{(q)}((X)^{(q)})$ are intrinsically defined as projective varieties in terms of the field $K=k((X)^{(q)})$. We have in fact the following general

PROPOSITION 7. *Let K be the field of rational functions of a complete non-singular variety V of dimension d. If* $\dim H^0(V,\Omega^{(d)})>0$, *then we can define the canonical image C of V. The variety C is determined with its structure of projective variety by the field K.*

The space of holomorphic d-forms of K is intrinsically defined (n. 4). Let $\Omega_1,\cdots,\Omega_\rho$ be a base of this space (ρ is certainly finite since the sheaf $\Omega^{(d)}$ is coherent).[15] Taking the Ω's as "homogeneous coordinates"[16] of a general point on a projective space $P_{\rho-1}$ we get as locus in $P_{\rho-1}$ the variety C. Since the Ω's are defined modulo a linear substitution, C is defined modulo a projective transformation. The definition depends solely on K.

6. Further properties of the canonical mappings. a) We give here some properties of the canonical mappings that will be needed later.

PROPOSITION 8. *Let C be the canonical image of a non-hyperelliptic curve. Then*

(α) *the tangent line t_P at the general point P of C is not tangent at any other point,*

(β) *the general hyperplane cuts C in $2g-2$ points such that any $g-1$ of them are linearly independent.*

---

[14] The image point $\phi^{(q)}((A_1)+\cdots+(A_q))$ may, however, be a singular point (for example, $g=4, q=2$).

[15] J. P. Serre [7, (a)].

[16] This means that we consider in the graded ring $k[X_1,\cdots,X_\rho]$ of homogeneous polynomials the ideal defined as the kernel of the homomorphisms given by $f(X_1,\cdots,X_\rho)\to f(\Omega_1,\cdots,\Omega_\rho)$ of $k[X_1,\cdots,X_\rho]$ into the ring of holomorphic tensor forms. The construction can also be described in the following form. We consider in K the rings $A_\iota=k[X_\iota^1,\cdots,X_\iota^\rho]$, where $X_\iota=\Omega_h/\Omega_\iota$, and we assume A_ι as ring of coordinates of the affine variety C_ι in the open set $U_\iota=\{y \mid y\in P_{\rho-1}, y_\iota\neq 0\}$ and we "put them together" by the change of coordinates $X_\iota^h=X_j^h/X_j^\iota$ to build up the variety C.

Proof of (α). Suppose t_P is tangent to C at the point $Q \neq P$. The specialty index of $2P+2Q$ is $i(2P+2Q)=g-2$, hence $\dim|2P+2Q|=2$. We have therefore a $g^2{}_4$ on C. This series gives a map of C on a plane quartic (since we cannot have $g^2{}_4 = 2g^2{}_2$ nor can the image be a conic since C is not rational). Hence the genus of C is $\leqq 3$.[17] This proves (α) for $g>3$.

If $g=3$, C is then a plane non-singular quartic. If t_P touches C also at $Q \neq P$, the dual curve Γ[18] of C will be a plane curve such that the general point t_P belongs to two different lines p, q (corresponding to P and Q) which meet Γ only at t_P. This implies that Γ is a line, i.e. the tangents to C will pass through the same point O (necessarily not on C). The lines containing O will give on C a series of type $2g^1{}_2$. This is impossible since C is not hyperelliptic.[19]

Proof of (β). The general hyperplane u cuts C in $2g-2$ distinct points. Suppose that $g-1$ of them are linearly dependent, i.e. the space spanned by $g-2$ of them contains the remaining point. There exists, therefore, an integer h such that $P_1,\cdots,P_h$ are linearly dependent while $P_1,\cdots,P_{h-1}$ are independent. Certainly $h \geqq 3$. Let $P_{g-1}{}^*$ be the dual space of P_{g-1} (the space of C), let G be the Grassmann manifold of subspaces of P_{g-1} of dimension $h-2$, and consider the irreducible correspondence T in $P_{g-1}{}^* \times G$ with the general point (u, space determined by $P_1,\cdots,P_{h-1}$). The principle of counting the constants[20] gives

$$\dim(P_{g-1}{}^*)+0=\dim T=\dim \mathrm{pr}_G(T)+g-h-2.$$

Therefore $\dim \mathrm{pr}_G(T)=h-1$. Now the variety on G whose general point represents the subspace of P_{g-1} of dimension $h-2$ spanned by $h-1$ independent general points of C has dimension $\leqq h-1$ and contains $\mathrm{pr}_G(T)$. It follows that our assumption implies that the general subspace spanned by $h-1$ independent general points contains another point of C (distinct from the given $h-1$).

Suppose that h is the minimum integer of this sort.

---

[17] J. P. Serre [7, (b)], Ch. IV, n. 8.

[18] The definition of the "dual curve" will be recalled at n. 10.

[19] We can also remark that if the tangent line at a generic point P of C is also tangent at Q, the series $P+Q$ is obtained by dividing by 2 the canonical series of C. But division of a linear series leads to a finite number of different results. (A. Weil, [9, (b)], p. 117). Hence we must have at least two couples $P+Q$, $P'+Q'$ without common points and linearly equivalent. This implies the existence on C of a $g^1{}_2$.

[20] W. V. D. Hodge and D. Pedoe [4], volume 2, p. 104.

If $h = 3$, then any line joining two general points of C meets C again in some other point. This implies that C has all tangent lines passing through the same point O.[21] The same will hold for a generic projection C' of C on a plane. Now C' is birationally equivalent to C.[22] The dual curve Γ of C' is a line. Moreover, the tangent line $t_{P'}$ at a general point of C' will not be tangent at any other point. This is because of α) and the fact that by generic projection the property is preserved, as we shall now prove. Consider the linear series cut out on C by the hyperplanes through a tangent line t_P; it is of dimension $g-3$ and degree $\leqq 2g-4$. The general divisor of this series cannot be obtained by taking p-times the general divisor of another linear series, because that would imply that C is hyperelliptic or rational. This shows that the property α) is maintained by the projection from a generic space lying in a hyperplane tangent to C at P but nowhere else. It appears now that $k(C')$ is a purely inseparable extension of $k(\Gamma)$ and hence that C' is rational. This is a contradiction.

If $h > 3$, take the projection C_0 of C from the space spanned by $h-3$ general independent points. We get a rational map $C \rightarrow C_0$ which is generally one to one because h is assumed to be minimal. Hence $k(C)$ is purely inseparable over $k(C_0)$, and therefore C and C_0 have the same genus.[23] Now for C_0, we have the following properties: i) each line joining two different general points on C_0 meets C_0 again in some other point; ii) the tangent line at a general point of C_0 is not tangent in any other point of C_0. This enables us to apply to C_0 the previous argument.

Remarks 1. From the argument given above, it follows that for a non-hyperelliptic curve X, the canonical map $\phi^{(q)}: (X)^{(q)} \rightarrow C^{(q)'}$ is rational and generally one to one if $1 \leqq q \leqq g-2$, so that $k((X)^{(q)})$ will be purely inseparable over $k(C^{(q)})$.

---

[21] E. Lluis [6]. Here we give a short proof. Let C be an algebraic curve in $P_r(k)$, $r \geqq 3$, P, Q being independent general points on C. Assume that all hyperplanes containing P and Q all contain a third point O of C. The point O must be different from P and Q since the general hyperplane is not tangent to C at P or Q. Add the coordinates of O to the ground field and consider the projection C' of C from O. The general point P' of C' is the projection of both P, Q. The tangent lines t_P, t_Q at P, Q respectively lie in the plane joining O to the tangent line $t_{P'}$ to C' at P'. This implies that t_P, t_Q have a point in common. Since P, Q are general and independent on C, it follows that the tangent lines at any two simple points of C must intersect. Since these lines do not belong to the same plane, they belong to the same point.

[22] This is an obvious consequence of the theorem on primitive elements, B. van der Waerden [8], p. 132.

[23] Suppose $k(C_0) = k(C)^{p^a}$. Denote by σ the automorphism of the universal domain given by exponentiation to the p^a-th power. If x, y are generators of $k(C)$ and $f(x,y) = 0$ is the equation they satisfy, $x\sigma$, $y\sigma$ are generators of $k(C)^{p^a} = k(C_0)$, and hence they satisfy the equation $f\sigma(x,y) = 0$. From this the assertion follows.

2. The above proof also gives *Clifford's theorem* (strong form): If the linear series g^r_n is special, then $n \geqq 2r$, and if $n = 2r$ either the series is the canonical series or else the curve is hyperelliptic.

Any divisor G_n of g^r_n has specialty index $i(G_n) = r - n - g$ (i.e. the canonical divisor containing G_n satisfies $r-n$ linearly independent linear conditions). Since g^r_n has dimension r we must have $i(G_n) \leqq g-r$. Hence $n \geqq 2r$.

Suppose now that the curve that carries the series is the canonical image of a non-hyperelliptic curve. Any r points $P_1 + \cdots + P_r$ may be completed in a positive divisor G_n of g^r_n. If $n = 2r$, then $i(G_{2r}) = g - r$ and, therefore, any hyperplane through $P_1, \cdots, P_r$, if these are linearly independent, will contain the full divisor G_{2r}. Since we suppose $r < g-1$, the above argument applies to give the result.

3. Another consequence of the proposition is that *the canonical curve C is a projectively normal variety.*

This is obvious if X is hyperelliptic since C is a rational normal curve. Suppose X non-hyperelliptic and denote by σ_k the dimension of the minimal sum $|K| + \cdots + |K|$ $k+1$ times, where $|K|$ is the canonical series. Let K_u be the general hyperplane section of C and A, B two disjoint sets of $g-2$ distinct points each, contained in K_u. We can find a hyperplane through A not containing any other point of K_u, and the same statement holds for B. Hence K_u gives at least $2g-3$ linearly independent conditions on the minimal sum $|K| + |K|$, i.e. $\sigma_1 - (2g-3) \geqq \sigma_0$. The same argument shows that there exists a hyperplane containing A, a hyperplane containing B and a third hyperplane containing a point P of K_u outside A and B such that the union of the three hyperplanes does not contain K_u. Hence $\sigma_2 - (2g-2) \geqq \sigma_1$, and similarly $\sigma_s - (2g-2) \geqq \sigma_{s-1}$. Since $\sigma_0 = g-1$ we get $\sigma_k \geqq 2(k+1)(g-1) - g$. By the theorem of R. R., we infer that the equality must hold.

b) Consider now in $(X)^{(g-1)} \times P_{g-1}{}^*$ the closed graph Φ of the canonical mapping, the space $P_{g-1}{}^*$ being identified with the dual of the space P_{g-1} of the canonical image C of X. Denote by u the point of $P_{g-1}{}^*$ which corresponds to the hyperplane $u = 0$ in P_{g-1}.

PROPOSITION 9. *Consider for $u \in P_{g-1}{}^*$ the set of corresponding points on $(X)^{(g-1)}$ (i.e. $\mathrm{pr}_{(X)^{(g-1)}}(\mathrm{pr}^{-1}_{P_{g-1}{}^*}(u) \cap \Phi)$).*

i) *If X is not hyperelliptic, this set consists of the points on $(X)^{(g-1)}$ corresponding to positive divisors of degree $g-1$ contained in the divisor cut out on C by the hyperplane $u=0$.*

ii) *If X is hyperelliptic this set corresponds to positive divisors on X which, by the canonical map: $X \to C$, are mapped onto the divisor cut out on C by the hyperplane $u=0$.*

Proof. i). For u a general point on P_{g-1}^*, the assertion follows from Proposition 8, (β). For any u, it follows from this by specialization. Here is the formal argument. Denote by $x^{(1)}, \cdots, x^{(g-1)}$ $g-1$ general independent points on P_{g-1}. Consider the projective variety W whose general point $z=z(x^{(1)}, \cdots, x^{(g-1)})$ has the homogeneous coordinates given by the coefficients of the polynomial in $v=(v^0, \cdots, v^{g-1})$, $\prod_{i=1}^{g-1} (x_0^{(i)}v^0 + \cdots + x_{g-1}^{(i)}v^{g-1})$. The variety W is a regular transform of the symmetric product $(P_{g-1})^{(g-1)}$, the mapping being strictly one to one. There exists therefore a regular and one to one mapping of $(X)^{(g-1)}$ into W. For our purposes, we may identify $(X)^{(g-1)} \times P_{g-1}^*$ with the corresponding image in $W \times P_{g-1}^*$.

Denote by $A_h = (a_0^{(h)}, \cdots, a_{g-1}^{(h)})$, $1 \leqq h \leqq 2g-2$, the points of the intersection of the general hyperplane $u=0$ with the canonical curve C. Consider the subvariety Ψ of $W \times P_{g-1}^*$ with general point $(z(A_1, \cdots, A_{g-1}), u)$. Since Φ is irreducible and since, by proposition 8, the points $((A_{i_1}) + \cdots + (A_{i_{g-1}}), u)$ all belong to Φ, it follows that the subvariety Ψ coincides with the image of Φ. Hence Ψ contains the points $(z(A_{i_1}, \cdots, A_{i_{g-1}}), u)$ ($(i_1, \cdots, i_{g-1})$ being a combination of the indices $1, \cdots, 2g-2$). Also those points are the only points with the second projection u.

Now by specialization $u \to u_0$, the points $A_1, \cdots, A_{2g-2}$ specialize in the points of the divisor $u_0=0$ on C. This specialization gives a unique specialization for the points considered on Ψ. Since Ψ is irreducible, any point of Ψ is a specialization of a general point and therefore the specialized points are the only point of Ψ with second projection u_0.

ii) The argument is the same. The only thing to be observed is that the correspondence defined for a general u in the statement is an irreducible correspondence. To do this, consider the regular natural map p: $(X)^{(g-1)} \to (C)^{(g-1)}$, and in $(C)^{(g-1)} \times P_{g-1}^*$, consider the irreducible correspondence T with general point $((A_1) + \cdots + (A_{g-1}), u)$, where $A_1 + \cdots + A_{g-1}$ is the divisor $u=0$ on C. The correspondence Φ is irreducible and contains the subvariety of $(X)^{(g-1)} \times P_{g-1}^*$ which is mapped by $(p, 1)$ onto T. This proves our assertion.

COROLLARY 1. *Let* $\hat{\Phi}$ *be the normalized model of the graph* Φ. *Then* Φ *is biregularly equivalent to the normalization of the canonical model* $P_{g-1}{}^*$ *in the field* $k((X)^{(g-1)})$.

This is an immediate consequence of Zariski's main theorem[24] since

α) $\hat{\Phi}$ is birationally equivalent to $(X)^{(g-1)}$ and locally normal,

β) $\hat{\Phi}$ is a projective variety and the projection $p\colon \hat{\Phi} \to P_{g-1}{}^*$ is regular,

γ) for any point $u \in P_{g-1}{}^*$, the inverse image $p^{-1}(u)$ is finite.

COROLLARY 2. *The canonical map* $\phi^{(g-1)}\colon (X)^{(g-1)} \to P_{g-1}{}^*$ *is regular at the point* $(A_1) + \cdots + (A_{g-1})$ *if and only if* $\dim |A_1 + \cdots + A_{g-1}| = 0$ *when* X *is not hyperelliptic. It is everywhere regular if* X *is hyperelliptic.*

Suppose X is not hyperelliptic. If $\dim |A_1 + \cdots + A_{g-1}| > 0$, all points $((A_1) + \cdots + (A_{g-1}), u)$, where $u = 0$ runs through all hyperplanes containing $A_1 + \cdots + A_{g-1}$, belong to the closed graph Φ of $\phi^{(g-1)}$. This shows that the set $((A_1) + \cdots + (A_{g-1})) \times P_{g-1}{}^* \cap \Phi$ is infinite and therefore $\phi^{(g-1)}$ cannot be regular at $(A_1) + \cdots + (A_{g-1})$.

Suppose X is hyperelliptic. The canonical image C of X is a rational normal curve with the general point, say, $(1, t, t^2, \cdots, t^{g-1})$. The canonical map $\phi^{(g-1)}$ may be factored into the regular natural map $(X)^{(g-1)} \to (C)^{(g-1)}$ and the map $(C)^{(g-1)} \to P_{g-1}{}^*$ given by

$$\begin{cases} u_h = \text{Det.} \begin{pmatrix} 1, t_1, \cdots, t_1{}^{h-1}, t_1{}^{h+1}, \cdots, t_1{}^{g-1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ 1, t_{g-1}, \cdots, t_{g-1}{}^{h-1}, t_{g-1}{}^{h+1}, \cdots, t_{g-1}{}^{g-1} \end{pmatrix} \\ 0 \leqq h \leqq g-1 \end{cases}$$

which associates to the general point $(t_1) + \cdots + (t_{g-1})$ on $C^{(g-1)}$ the hyperplane containing the points $t_1, \cdots, t_{g-1}$ of C.

This second map is also regular. Computing the determinant, we find the value $\phi_{g-h-1}(t_1, \cdots, t_{g-1}) W(t_1, \cdots, t_{g-1})$,[25] where ϕ_α is the elementary symmetric function of degree α and W the Vandermonde determinant in the quantities $t_1, \cdots, t_{g-1}$. The mapping may thus be written as

$$u_h = \phi_{g-h-1}(t_1, \cdots, t_{g-1}), \qquad 0 \leqq h \leqq g-1,$$

and this proves the assumption.

---

[24] O. Zariski [10], p. 82.

[25] The determinant vanishes if W vanishes. Also, it vanishes if ϕ_{g-h-1} vanishes since this is the condition that $t_1, \cdots, t_{g-1}$ be the roots of an equation of degree $g-1$, $a_{g-1}x^{g-1} + \cdots + a_{h-1}x^{h-1} + a_{h+1}x^{h+1} + \cdots + a_0 = 0$. Hence it is divisible by $\phi_{g-h-1}W$ and hence equals this product.

Section 3. The theorem of Torelli.

7. The branch locus of a rational map. a) Let $f\colon X \to P$ be a rational map of a projective irreducible variety of dimension d on a projective space P_d, i. e. $f^*\colon k(P) \to k(X)$ is a monomorphism and hence $k(X)$ is an algebraic extension of $k(P)$. We will suppose the extension a separable one, i. e. that the map f is separable.

Denote by Φ the closed graph of f, that is, the projective subvariety of $X \times P$ with general point $(x, f(x))$, where x is general point on X. We have $\mathrm{pr}_X(\Phi) = X$, $\mathrm{pr}_P(\Phi) = P$, since X and P are complete. Given a point $y \in P$, $f^{-1}(y)$ will denote the set of points $\mathrm{pr}_X(\Phi \cap X \times y)$.

b) LEMMA 1. *The points $y \in P$ such that $f^{-1}(y)$ is not finite are contained in an algebraic variety of dimension $\leqq d - 2$.*[26]

Let $(y_0, \cdots, y_d)$ be homogeneous coordinates on P, denote by U_i the open set $y_i \neq 0$ and identify it with k^d where $\xi_1, \cdots, \xi_d$ are coordinates. Let V_j be a finite affine open covering of X and let $(z_1, \cdots, z_r)$ be the coordinates on V_j. The z_i's satisfy algebraic equations $a_0^{(i)}(\xi) z_i^{n_i} + \cdots + a_{n_i}^{(i)}(\xi) = 0$, where the a's may be supposed in $k[\xi]$ and without common factors. If ξ does not satisfy the equations $a_k^{(i)}(\xi) = 0$, then $f^{-1}(\xi) \cap V_j$ is finite. The locus W_{ij} defined by the equations $a_k^{(i)}(\xi) = 0$ is of dimension $\leqq d - 2$. Therefore, $f^{-1}(y)$ will be finite if $y \notin \cup \bar{W}_{ij}$.

LEMMA 2. *There are points $y \in P$ such that $f^{-1}(y)$ is finite and consists of $n = [k(X) : k(P)]$ different points. These points y cover an open set in P.*

Let V be an affine open set on X with coordinates $z_1, \cdots, z_r$. We may suppose that each z_i, as an element of $k(X)$, is such that $k(P)(z_i) = k(X)$. With the same notation as above, we have irreducible equations

$$F_i \equiv a_0^{(i)}(\xi) z_i^n + \cdots + a_n^{(i)}(\xi) = 0$$

of the same degree $n = [k(X) : k(P)]$. Moreover, since $k(\xi, z_i) = k(\xi, z_j)$, we have rational expressions of the type: $z_i = R_{ij}(\xi, z_j) = P_{ij}(\xi, z_j)/Q_{ij}(\xi, z_j)$, where P, Q are polynomials in their arguments, and where Q_{ij} is prime to F_j. Hence the above expression may be written in the form $z_i = P_{ij}(\xi, z_j)/Q_{ij}(\xi)$. Now suppose that $y \in U$ does not satisfy any one of the equations $\Pi Q_{ij}(\xi) = 0$,

---

[26] The lemma holds for any rational map $f\colon X \to Y$ between algebraic manifolds of the same dimension d (there always exists a regular map $\phi\colon Y \to P_d$. Then apply the lemma to $\phi \circ f$).

$\Pi a_0^{(i)}(\xi) = 0$, Discriminant $(F_i) = 0$. It follows that the equations F_i have n distinct roots, and because of the above relations, there are n distinct points that correspond to y on V. Since any finite set of points can be covered with an open affine set the assertion follows.

Let A be the set of points $y \in P$ such that $f^{-1}(y)$ consists of n distinct points. The minimal algebraic variety containing the complement of A (i.e. the closure of the complement of A) will be denoted by D.

LEMMA 3. *Let X, X' be two projective and locally normal varieties birationally equivalent; hence $k(P) \subset k(X) = k(X')$. The loci D, D' relative to the corresponding rational maps $f: X \rightarrow P$, $f': X' \rightarrow P$ differ at most on a variety of dimension $\leqq d-2$.*

Going to the graph of the birational map $\phi: X \rightarrow X'$, we may suppose that ϕ is regular (we have to take the normalized model of the graph). Now since X, X' are locally normal, ϕ is a one to one map outside of a subvariety $W' \subset X'$ of dimension $\leqq d-2$ (n. 4, Lemma 1). Since the definition of D (by means of the sets $f^{-1}(y)$, $y \in P$) involves only the graph of the mapping f, we may as well suppose f (and f') regular. From this, the assertion follows.

The pure part of dimension $d-1$ of D has an intrinsic meaning in terms of the extension $k(P) \subset k(X)$ and the chosen model P of $k(P)$. It will be called the *branch locus* of the rational map $f: X \rightarrow P$.

Remarks. 1. The branch locus can be equally defined for a non-separable algebraic extension of $k(P)$ by substituting the given extension $k(X)$ with the maximal separable extension L of $k(P)$ in $k(X)$ and applying the above definition to L.

2. The branch locus can also be described in terms of valuations: it is the divisor corresponding to the valuations of the ring of coordinates of the affine model $U_i \subset P$ which are ramified in the extension field $k(X)$ of $k(U_i)$, $0 \leqq i \leqq d$.

8. The branch locus for the canonical map f: $(X)^{(g-1)} \rightarrow P^*_{g-1}$. We identify (as in n. 5, e)) the space P_{g-1}^* with the dual space of the space P_{g-1} of the canonical image C of the curve X. Let D be the branch locus of the canonical map f.

PROPOSITION 10. i) *If X is not hyperelliptic, D is irreducible, and a* *general point of D is given by the general tangent hyperplane to the canonical curve.*.

ii) *If X is hyperelliptic, the locus D consists again of the irreducible hypersurface of the tangent hyperplanes to C and of the hyperplanes which represent the stars of hyperplanes in P_{g-1} with center at the branch points on C (for the canonical map $\phi\colon X \to C$).*

i) Since X is not hyperelliptic, X may be identified with the curve C whose order is $2g-2$ ($g =$ genus of X). If $y \notin D$, D being the set described in the proposition, then $f^{-1}(y)$ consists of exactly $\binom{2g-2}{g-1}$ different points; if $y \in D$, then $f^{-1}(y)$ consists of at most $\binom{2g-2}{g-1} - \binom{2g-4}{g-2}$ different points. Since $(X)^{(g)}$ is locally normal, this characterizes D as the branch locus if we prove that D is pure (in fact, irreducible) of dimension $g-2$.

ii) In an analogous way, if X is hyperelliptic, the same argument applies to the locus D described in the proposition (in this case, for $y \notin D$, $f^{-1}(y)$ consists of 2^{g-1} distinct points). The proof will be completed if we prove the following:

LEMMA. *Let C be a non-singular algebraic curve belonging to some projective space P_n with $n \geqq 2$; the hyperplanes tangent to C are represented by the points of an irreducible hypersurface in the dual space P^* of P.*

Denote by $(1, \xi_1, \cdots, \xi_n)$ a general point of C and let $(u_0, \cdots, u_n)$ be homogeneous coordinates on P^*. We may suppose $k(C)$ is a separable extension of $k(\xi_1)$. The two quantities:

$$\begin{aligned} u_0 &= -\{u_1\xi_1 + \cdots + u_n\xi_n\} \\ &\qquad = -\{u_2(\xi_2 - d\xi_2/d\xi_1)\xi_1) + \cdots + u_n(\xi_n - d\xi_n/d\xi_1)\xi_1)\} \\ u_1 &= -\{u_2(d\xi_2/d\xi_1) + \cdots + u_n(d\xi_n/d\xi_1)\} \end{aligned}$$

(which give the conditions for the hyperplane $(u_0, \cdots, u_n)$ to be tangent to C) are algebraically dependent over $k(u_2, \cdots, u_n)$. Hence we have an algebraic equation $F(u_0, u_1, u_2, \cdots, u_n) = 0$. This equation is unique since u_1 or u_2 is transcendental over $k(u_2, \cdots, u_n)$. Suppose, in fact, that this is not the case. Then the quantities $c_i = d\xi_i/d\xi_1$, $2 \leqq i \leqq n$, are constant because u_1 is algebraic over $k(u_2, \cdots, u_n)$. The qualities $d_i = \xi_i - c_i\xi_1$, $2 \leqq i \leqq n$, are also constant for an analogous reason. This implies that C is a line, which is excluded by hypothesis.

We may suppose that F is a polynomial in all the u's and irreducible, not only as a polynomial in u_0, u_1 but in all the variables. This polynomial F

is certainly homogeneous. In fact, if u satisfies $F(u)=0$, then λu must satisfy $F(\lambda u)=0$ for a general parameter λ; since $F(u)$ is irreducible and of the same degree in the u's as $F(\lambda u)$, we must have $F(\lambda u)=A(\lambda)F(u)$ with $A(\lambda)$ a polynomial in λ alone and in fact $=\lambda^{\text{degree of } F}$.

Hence the coordinates of the general tangent plane satisfy the equation $F(u)=0$. But C is non-singular; therefore, any tangent plane may be obtained by specialization from the general.[27] This proves the lemma.

9. Proof of Torelli's theorem for characteristic $p=0$.

We recall the statement of the theorem:

THEOREM 1. *If the symmetric products* $(X)^{(g-1)}$, $(Y)^{(g-1)}$ *of two curves* X, Y *of the same genus* g *are birationally equivalent, then the curves* X, Y *are also birationally equivalent.*

From the hypothesis $k((X)^{(g-1)})=k((Y)^{(g-1)})$, it follows that the branch locus D in the canonical model $P_{g-1}{}^*$ is the same for both symmetric products. From the reducibility or not of the hypersurface D, we infer that both X, Y are hyperelliptic or not. We consider separately the two cases.

(a) *Non-hyperelliptic case.* From the description of the locus D given in the previous n. 7, it follows that the canonical curves C and Γ, of X and Y respectively, have the same set of tangent hyperplanes. The plane projections C', Γ' of C, Γ from a general projective subspace of dimension $g-4$ have therefore the same set of tangent lines. We conclude from that (since we are in characteristic $p=0$) that $C'=\Gamma'$. Since $k(X)=k(C)=k(C')$ and $k(Y)=k(\Gamma)=k(\Gamma')$, we have $k(X)=k(Y)$. q.e.d.

(b) *Hyperelliptic case.* Since the characteristic p is $\neq 2$, any hyperelliptic curve X corresponds to a quadratic extension $k(x,y)$ of $k(x)$, where $y^2=\prod_{i=1}^{2g+2}(x-\alpha_i)$ with $\alpha_i\neq\alpha_j$, and it is therefore uniquely determined by the $2g+2$ branch points $x=\alpha_i$. Moreover, the field $k(x)$ may be identified with the field of the canonical image of the given curve so that the curve X will be determined by the knowledge of its canonical image C and the position on it of the $2g+2$ branch points. We may also remark that in fact, the $2g+2$ branch points above are able to determine the curve X since they will determine automatically the unique normal rational curve C which contains them.[28]

---

[27] Let $a=(a_0,\cdots,a_n)$ be a point of C; suppose for instance, $a_0\neq 0$ and that x_1 is a uniformizing parameter at a; specializing $\xi_i\to a_i/a_0$, the derivatives $d\xi_i/d\xi_1$ are specialized into finite quantities t_i; the specialized hyperplanes given by the above relations continue to satisfy $F(u)=0$.

Now again the branch locus D is the same for the two products $(X)^{(g-1)}$, $(Y)^{(g-1)}$. Moreover, D consists of an irreducible hypersurface of order > 1[29] representing the tangent hyperplanes to a rational normal curve of P_{g-1} and of $2g+2$ hyperplanes. These hyperplanes determine in P_{g-1} the $2g+2$ branch points on the canonical image of X and of Y. The theorem follows from the above remarks.

Remark. If X, Y, and the given birational map $(X)^{(g-1)} \rightarrow (Y)^{(g-1)}$ are all defined over a field $k_0 \subset k$, then the birational map $X \rightarrow Y$ is also defined over k_0.

This follows from the proof, since by a linear transformation over k_0, the canonical images (and the branch set on them in the hyperelliptic case) can be superposed.[30]

The remark is useful, in the case $k_0 = \boldsymbol{R}$ is the real field. It gives a *Torelli theorem for* the existence of *conformal mapping* of a Riemann surface with boundaries into another with the same genus and the same number of connected boundaries.

10. Some remarks, not indispensable, for the case of characteristic $p \neq 2$. a) We want to show that the above proof essentially holds true for any characteristic $p \neq 2$.

Note first that, in the hyperelliptic case, nothing has to be changed. In the non-hyperelliptic case, we have to investigate to see if the set of tangent lines at the non-singular points of an irreducible algebraic plane curve are able to determine the curve uniquely. Since the question is of a local nature, we may suppose the given curve C to be the locus of a general point (x, y) in the affine plane. Let $f(x, y) = 0$ be the equation of C. The tangent line at (x, y), $(X - x)\partial f/\partial x + (Y - y)\partial f/\partial y = 0$, has the coordinates

---

[28] A rational normal curve C in P_n is uniquely determined by any $n+3$ distinct points of it. Cf. Bertini, Complementi di Geometria Proiettiva, Zanichelli, Bologna (1927), p. 67.

[29] This again because $p \neq 2$.

[30] Notice that the genus of X, Y does not change by extending the field of constants from k_0 to k, hence the linear spaces of differentials over X, Y and on the symmetric product all have the same dimension as over k so that the canonical mappings are defined over k_0. (See the book of C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, American Math. Soc. (1951); in particular, Theorem 4, p. 30 and Theorem 5, p. 99).

$(-\{x\partial f/\partial x+y\partial f/\partial y\},\partial f/\partial x,\partial f/\partial y)$. Suppose for instance $\partial f/\partial y\neq 0$; then the rational functions

$$-(y-x(\partial f/\partial x)/(\partial f/\partial y))=U,\qquad -(\partial f/\partial x)/(\partial f/\partial y)=V$$

are the coordinates of a general point of a curve Γ (if C is not a line[31]) called the "dual curve of C" or the "envelope of C." We have a rational map $\phi\colon C\rightarrow\Gamma$ given by the above formulae, which maps a general point of C in a general point of Γ.

LEMMA. *Let P be the center on C of a linear branch with tangent $l_P=0$. Suppose $v_P(l_P)=q\not\equiv 0\pmod p$. Then to this branch, ϕ associates a branch on Γ of lines, with center at $l_P=0$ and with contact point on $l_P=0$ at the point P.*

Suppose P at the origin with tangent there in $y=0$. The given branch has an expansion of the type $y=c_qx^q+c_{q+1}x^{q+1}+\cdots$ with $c_q\neq 0$. The transformed branch has the equations:

$$U=(q-1)c_qx^q+qc_{q+1}x^{q+1}+\cdots$$

$$V=-\{qc_qx^{q-1}+(q+1)c_{q+1}x^q+\cdots\}.$$

The contact point has the coordinate $x_c=(U/V)_{x=0}$; hence the assertion is proved.

COROLLARY. *If for a point P of $C, v_P(l_P)=2$, then for the general point Q of $C, v_Q(l_Q)=2$ and, if the characteristic p is not 2, the map ϕ is birational.*

We can take as general point the point $Q=\left\{\begin{smallmatrix}x=\alpha\\ y=\Sigma c_r\alpha^r\end{smallmatrix}\right.$ (in the field $k\{\{\alpha\}\}$ of power series with finite negative powers). If $q=2$, then one easily verifies $v_Q(l_Q)=2$. Moreover, the above lemma shows that if for the general point P, $v_P(l_P)=q$ is not divisible by p, then the coordinates of P are rational functions of the coordinates of the general point of Γ.[32]

b) To complete our argument, we have only to show that the general projection C' of the canonical image of a non-hyperelliptic curve X is in the condition of the corollary.

Now if C is an algebraic curve in P_r and C' is its general plane projection, the mapping $C \rightarrow C'$ is birational. Denote by P, P' corresponding general points on C, C' and by $l = 0$, $l' = 0$ the corresponding tangent hyperplane and tangent line. Then $v_P(l) = v_{P'}(l')$. All this is an obvious consequence of the theorem on primitive elements.

---

[31] In homogeneous coordinates, if $\partial f/\partial x_i=\rho c_i$ with $c_i\in k$ and $\rho\neq 0$. From the Euler formula $\sum(\partial f/\partial x_i)x_i=0$, we get for the general point x of C, $\sum c_ix_i=0$.

[32] Hence for a general point P of C either $v_P(l_P)$ is divisible by the characteristic p or $v_P(l_P)=2$.

For values of the genus $g \geqq 4$, we have the following:

PROPOSITION 11 . *Let C be the canonical image of a non-hyperelliptic curve of genus $g \geqq 4$. Let P be a generic point on C and let $l_P = 0$ be the general tangent hyperplane to C at P. Then $v_P(l_P) = 2$.*

Suppose $v_P(l_P) \geqq 3$. The specialty index of the divisor $3P$ is therefore $i(3P) = g - 2$. The linear series $|3P|$ has dimension 1.[33] Let ϕ be a non-constant rational function with the pole $3P$: $(\phi) \succ -3P$. The field $k(C)$ is a separable extension of $k(\phi)$ with $[k(C) : k(\phi)] = 3$. (If the extension were inseparable C would be rational.) Take another point Q such that $v_Q(\phi - \phi(Q)) \neq 3$; this forbids only a finite number of positions for Q since $k(C)/k(\phi)$ is separable. If for Q we have $v_Q(l_Q) \geqq 3$, then we have another rational function ψ, non-constant, with $(\psi) \succ -3Q$. Again $k(C)$ is a separable extension of degree 3 of $k(\psi)$. The composition field of $k(\phi)$ and $k(\psi)$ is $k(C)$ itself, since $k(\phi) \neq k(\psi)$ in $k(C)$. We apply the following remark:

Let $K = k(X)$ be the field of rational functions on an algebraic curve X. Suppose that $K = k(\phi, \psi)$ with $[K : k(\phi)] = n$, $[K : k(\psi)] = m$ (both extensions being separable). Then the genus of $X \leqq n \cdot m - n - m + 1$.[34]

If we apply this to $X = C$ for $n = m = 3$, we get the proposition for the values $g > 4$.

For $g = 4$, C is a curve which belongs to a surface F of second order in P_3 (as it is shown by the theorem of R. R.). The groups of the series $|3P|$, since $i(3P) = g - 2 = 2$, belong to lines necessarily contained in F. Hence we cannot have on C more than 2 series of order 3 and dimension 1.

This settles the case $g \geqq 4$ (for characteristic $p \neq 2$). For the case $g = 3$, we have to consider only the case of characteristic $p = 3$ when all tangents to the canonical plane quartic curve are all inflection lines. This can be done as in a paper of L. Gauthier.[35]

---

[33] "Projective dimension," i. e. $l(3P) = 2$.

[34] J. P. Serre [7, (b)], Ch. IV, n. 8.

[35] L. Gauthier [3]. Any such quartic, by suitable choice of homogeneous coordinates x_0, x_1, x_2, can be brought into the form $x_1 x_2^3 + x_2 x_0^3 + x_0 x_1^3 = 0$. On this curve, the verification becomes obvious.

11. Proof of the theorem for the non-hyperelliptic case. We give here the proof of Torelli's theorem, valid for any characteristic p for the case in which the curves we consider are not hyperelliptic.

LEMMA. *The rational map* $\phi\colon C' \to \Gamma$ *(of the general plane projection* C' *of the canonical curve* C *onto its envelope* Γ*) is purely inseparable.*

This is an obvious consequence of Proposition 8.

Suppose now we have two curves C', C'' with the same envelope Γ; we want to show that C' and C'' are birationally equivalent.

Suppose $[k(C'):k(\Gamma)] = p^{\alpha'}$, $[k(C''):k(\Gamma)] = p^{\alpha''}$ so that $k(C')^{p^{\alpha'}} = k(\Gamma)$, $k(C'')^{p^{\alpha''}} = k(\Gamma)$. Suppose $\alpha' \geqq \alpha''$; then $k(C'') = k(C')^{p^{\alpha'}-p^{\alpha''}}$. We have to prove that in fact $\alpha' = \alpha''$. To do this, denote by σ the automorphism of the universal domain Ω given by the exponentiation to the power $p^{\alpha'-\alpha''}$. We have $k(C')^{\sigma} = k(C'')$. If $f(x', y') = 0$ is the equation of C', $f^{\sigma}(x'', y'') = 0$ will be the equation of C''. If M' is a general point of C', $M'' = M'^{\sigma}$ is a general point of C''. Now $k(\Gamma)$ is defined as the field

$$k(y' - x'(\partial f/\partial x')/(\partial f/\partial y'), (\partial f/\partial x')/(\partial f/\partial y')),$$

the generators being computed at M'. Applying the automorphism σ, we get the field

$$k^{\sigma}(y'' - x''\{(\partial f/\partial x')/(\partial f/\partial y')\}^{\sigma}, \{(\partial f/\partial x')/(\partial f/\partial y')\}^{\sigma}).$$

Now $k^{\sigma} = k$ since k is perfect; moreover, $(\partial f/\partial x')^{\sigma} = \partial f^{\sigma}/\partial x''$ $(\partial f/\partial y')^{\sigma} = \partial f^{\sigma}/\partial y''$ (these partial derivatives being computed at $M'' = M'^{\sigma}$). Hence σ carries the extension $k(C')/k(\Gamma)$ over the extension $k(C'')/k(\Gamma)$. Hence we must have $p^{\alpha'} = p^{\alpha''}$. q. e. d.

12. Proof of the theorem for the hyperelliptic case. a) We have already remarked that the proof given for characteristic $p = 0$ holds without changes for any characteristic $p \neq 2$.

For $p = 2$, there is no hope to deduce the theorem from the knowledge of the branch set on the canonical image. In this case, we have to deal with a quadratic extension $K(y)$ of the field $K = k(x)$ generated by an equation of type $y^2 - y = Q(x)$, where $Q(x) \in k(x)$ is determined mod. a substitution of type $Q(x) \to Q(x) + Q_0{}^2(x) - Q_0(x)$ with $Q_0(x) \in k(x)$. The rational function $Q(x)$ may be assumed in the form $Q(x) = A(x)/B(x)$ with A, B in $k[x]$ without common factors and such that every prime divisor of B is of odd multiplicity. The knowledge of the branch set gives the prime divisors of B which is utterly insufficient.

b) To prove the theorem in this case, we make the following remarks:

(α) For a hyperelliptic curve X the model $(X)^{(g-1)}$ is intrinsically defined with respect to biregular transformations in terms of the field $k((X)^{(g-1)})$.

In fact, since the canonical mapping is regular (Proposition 9, Corollary 2), $(X)^{(g-1)}$ is biregularly equivalent to the graph Φ of the mapping. Now Φ is non-singular, hence locally normal, therefore Φ coincides with its own normalized model Φ. Because of Corollary 1 to Proposition 9, we have proved the assertion.

(β) The canonical system on $(X)^{(g-1)}$ has a fixed part in the subvariety which is the locus of the point $(P_1) + (P_1^\sigma) + (P_3) + \cdots + (P_{g-1})$, where $P_1, P_3, \cdots, P_{g-1}$ are general independent points on X and σ is the automorphism of X into itself given by the $g^1{}_2$. (In the notation above, for $p = 2$, $\sigma\colon (x, y) \rightarrow (x, y+1)$). This follows from Proposition 6.

Consider now the canonical map $\phi\colon (X)^{(g-1)} \rightarrow P_{g-1}{}^*$. The points $y \in P_{g-1}{}^*$ such that $\phi^{-1}(y)$ has the minimum number of distinct points are given by the images of the osculator hyperplanes to the canonical image C of X. The curve C is rational normal, and the osculator hyperplane at any point $P \in C$ is uniquely determined and meets C only at P. The locus of the points y is therefore a rational curve Γ of $P_{g-1}{}^*$.

The set $\phi^{-1}(\Gamma)$ consists of the curves Δ_h, $0 \leqq h \leqq [(g-1)/2]$, which are the images on $(X)^{(g-1)}$ of the curve X by the mappings $f_h\colon Q \rightarrow h(Q) + (g-1-h)Q$. Only Δ_0, i.e. the diagonal of $(X)^{(g-1)}$, does not lie on the common part of the canonical system. Notice also that $[k(X) : k(\Delta_0)] = p^{\alpha}$[36] for some $\alpha \geqq 0$. Suppose now that for the curve Y, we have $k((Y)^{(g-1)}) = k((X)^{(g-1)})$. Then we have a biregular map of $(Y)^{(g-1)}$ onto $(X)^{(g-1)}$. Hence the diagonal Δ_0' of $(Y)^{(g-1)}$ is birationally equivalent with the diagonal Δ_0 of $(X)^{(g-1)}$. Moreover, the same argument given in n. 11 shows that $[k(Y) : k(\Delta_0')] = [k(X) : k(\Delta_0)]$.[37] This proves that $k(Y) \approx k(X)$.

q. e. d.

An analogous remark applies here as at the end of n. 9 (k_0 perfect).

---

[36] Actually p^α = greatest power of p dividing $g-1$ (cf. J. P. Serre [7, (b)], Ch. III, n. 14).

[37] Or because both degrees equal the greatest power of p dividing $g-1$.

REFERENCES.

[1] P. Cartier, "Calcul Différentiel sur les Variétés Algébriques en Caractéristique non Nulle," *Comptes Rendus Hebdomaires des Séances de l'Académie des Sciences*, Paris, vol. 245 (1957), pp. 1109-1111.

[2] S. Eilenberg and J. A. Zilber, "On product of complexes," *American Journal of Mathematics*, vol. 75 (1953), pp. 200- 204.

[3] L. Gauthier, to appear in *Journal de Mathématiques Pures et Appliquées.*

[4] W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, Cambridge University Press, 1952.

[5] S. Koizumi, "On the differential forms of the first kind on algebraic varieties," *Journal of the Mathematical Society of Japan*, vol. 1, n. 3 (1949), pp. 273-280, and vol. 2, n. 4 (1951), pp. 267-269.

[6] E. Lluis, "De las Singularitades que Aparecen al Projectar Varietades Algebricas," *Boletin de la Sociedad Matematica Mexicana*, vol. 1, s. 2, n. 1 (1956), pp. 1-9.

[7] J. P. Serre, (a) "Faisceaux Algébriques Cohérents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.

———, (b) *Groupes Algébriques et Théorie du Corps de Classes*, College de France's lectures, 1957.

[8] B. van der Waerden, *Moderne Algebra*, Springer, Berlin, 1940.

[9] A. Weil, (a) *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, 1946.

———, (b) *Variétés Abéliennes et Courbes Algébriques*, Hermann, Paris, 1948.

———, (c) "Zum Beweis des Torellischen Satzes," *Nachrichten der Akademie Wissenschaften in Göttingen* (1957), pp. 33-53.

[10] O. Zariski, "The Fundamental Ideas of Abstract Algebraic Geometry," *Proceedings of the International Congress of Mathematicians*, vol. 2 (1950), pp. 77-89.

THE SPECTRA OF MULTIPLIER TRANSFORMS ON l^p.*

By A. Devinatz and I. I. Hirschman, Jr.[1]

1. Introduction. In this paper, we consider spectral problems for multiplier transforms defined on the sequence spaces l^p, $1 \leqq p \leqq \infty$. We collect the basic and elementary facts about these operators in § 2. We show that to every such operator T on l^p there corresponds a unique (a. e.), bounded, measurable function $T^\wedge(\theta)$ defined on the interval $[0, 1]$. The converse is not necessarily true, except for $p = 2$.

In § 3, we characterize a wide class of functions $T^\wedge(\theta)$ for which the spectrum of the corresponding multiplier transform T is the essential range of the function. This means that the spectrum of any such operator does not change when it is considered as acting different l^p. However, the point spectrum may change as p changes. In § 4, we give some theorems which lead to a characterization of the point spectrum of certain classes of operators in terms of sets of multiplicity for l^p. We also give an example which shows the change of point spectrum as p changes. In so doing, we partially answer, in the negative, a question posed by P. Hartman [2]. We close the paper in § 5 with two theorems which are closely connected with the problem of spectral synthesis in l^∞.

2. Preliminaries. We shall designate by l^p, $1 \leqq p < \infty$, the Banach space of sequences of complex numbers such that

$$\| a \|_p = [\sum_{-\infty}^{\infty} | a(n) |^p]^{1/p} < \infty.$$

By l^∞, we shall designate the bounded sequences with

$$\| a \|_\infty = \sup_n | a(n) |,$$

by l_0^∞, the subspace of l^∞ whose elements vanish at infinity, by l_0, the sequences which vanish off a finite set of integers, and by l, the class of all sequences.

---

* Received November 11, 1957.

[1] This research was partially supported by the United States Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF18(600)-568. Reproduction in whole or in part is permitted for any purpose of the United States Government.

For $a, b \in l$ we shall write

$$a * b(n) = \sum_{k=-\infty}^{\infty} a(n-k) b(k),$$

whenever this is defined for all n. Also, we set

$$(a, b) = \sum_{-\infty}^{\infty} a(n) b(-n),$$

whenever this is defined. For future reference, we note that if $a, c \in l_0$, $b \in l$, then

$$(a * b, c) = (a, b * c).$$

If p and q are conjugate indices,[2] then (a, b) is a bilinear functional on $l^p \times l^q$ which satisfies the relation

$$|(a, b)| \leqq \| a \|_p \| b \|_q.$$

For fixed b, (a, b) is a continuous linear functional on l^p. Moreover, if $a \in l^p$, $1 \leqq p \leqq \infty$, then

$$\| a \|_p = \operatorname*{l.u.b.}_{b \in l_0, \| b \|_q = 1} |(a, b)|. \tag{2.1}$$

A linear transform T with domain l_0 and range in l which satisfies

$$T(a * b) = T(a) * b$$

for every $a, b \in l_0$ will be called a multiplier transformation. Let e be the identity element of l; i.e. $e(0) = 1$, $e(n) = 0$ if $n \neq 0$. Then for any $a \in l_0$,

$$T(a) = T(e * a) = T(e) * a = t * a, \tag{2.2}$$

where $t = Te$. Let

$$\| T \|_p = \text{l. u. b.} \| Ta \|_p / \| a \|_p, \qquad (1 \leqq p \leqq \infty), \tag{2.3}$$

the least upper bound being extended over all $a \in l_0$ except $a = 0$. If $1 \leqq p < \infty$, then l_0 is dense in l^p while if $p = \infty$, then l_0 is dense in l_0^∞; thus if $\| T \|_p$ is finite, T has a unique extension as a bounded linear transformation of l^p to itself for $1 \leqq p < \infty$ and of l_0^∞ to itself if $p = \infty$. Let us denote by $\mathfrak{J}(T)$ the set of indices p for which $\| T \|_p$ is finite. We first assert that if $p_1, p_2 \in \mathfrak{J}(T)$ and if $1/r = (1 - \omega)(1/p_1) + \omega(1/p_2)$, where $0 < \omega < 1$, then $r \in \mathfrak{J}(T)$ and $\| T \|_r \leqq \| T \|_{p_1}^{1-\omega} \| T \|_{p_2}^{\omega}$. This is an application of the Riesz-Thorin convexity theorem. We next assert that if $p \in \mathfrak{J}(T)$

---

[2] By this, we mean $1/p + 1/q = 1$. We shall always use p and q to designate conjugate indices.

then the conjugate index $q \in \mathfrak{F}(T)$ and $\| T \|_p = \| T \|_q$. To see this, we note that if $a, b \in l_0$, then

$$(Ta, b) = (a * t, b) = (a, t * b),$$

and thus

$$|(Ta, b)| \leqq \| a \|_q \| t * b \|_p \leqq \| a \|_q \| T \|_p \| b \|_p.$$

Referring to (2.1) and (2.3), we see that $\| T \|_q \leqq \| T \|_p$. Since the roles of p and q can be reversed, we have $\| T \|_p \leqq \| T \|_q$, and thus $\| T \|_p = \| T \|_q$ as desired.

These two remarks show that if $\mathfrak{F}(T)$ is not empty, then it is an interval (open or closed) with end points $1 \leqq \mu \leqq \nu \leqq \infty$ which satisfy $1/\mu + 1/\nu = 1$. In particular, if $\mathfrak{F}(T)$ is not empty, then $2 \in \mathfrak{F}(T)$. We also note that the convexity and conjugacy properties described above imply that if $p \in \mathfrak{F}(T)$, then $\| T \|_p \geqq \| T \|_2$.

If $p \in \mathfrak{F}(T)$, then, as we have remarked, $q \in \mathfrak{F}(T)$, where q is the index conjugate to p. Thus, $Te = t$ belongs to l^q. By (2.2) $Ta = t * a$ for any $a \in l_0$. Using the fact that $t \in l^q$, it is easily seen that this formula holds for $a \in l^p$ if $1 \leqq p < \infty$ and for $a \in l_0{}^\infty$ if $p = \infty$. If $p = \infty$, so that $t \in l^1$, then the right side of the formula $Ta = t * a$ is meaningful for $a \in l^\infty$ and in fact provides a natural extension of T from $l_0{}^\infty$ to l^∞, which we continue to denote by T. T considered as a transformation from l^∞ to l^∞ clearly has the same norm as T considered as a transformation from $l_0{}^\infty$ to $l_0{}^\infty$ (this latter is of course just $\| T \|_\infty$).

If $\mathfrak{F}(T)$ is not empty, then, since $2 \in \mathfrak{F}(T)$, $Te \in l^2$ and we get

$$t(n) = Te(n) = \int_0^1 e^{-2\pi i\theta} t^\wedge(\theta)\, d\theta.$$

Here,

$$t^\wedge(\theta) = \sum_{-\infty}^{\infty} t(n) e^{-2\pi i n\theta} \qquad (\mathfrak{M}_2),$$

the symbol $\mathfrak{M}_2$ indicating that $t^\wedge(\theta)$ is a limit in the mean of order 2 of the partial sums of the series on the right. It is well known and easily obtained by standard arguments that $\| t^\wedge \|_\infty = \| T \|_2$, where $\| t^\wedge \|_\infty =$ essential sup $| t^\wedge(\theta) |$. Therefore, an earlier remark gives

$$(2.4) \qquad \| t^\wedge \|_\infty \leqq \| T \|_p \qquad p \in \mathfrak{F}(T).$$

3. The spectrum of multiplier transforms. Let T_1 and T_2 be multiplier transforms on l^p, $p \in \mathfrak{F}(T)$, and let $T = T_1 T_2$. It is easily seen that, with an evident choice of notations, $t^\wedge(\theta) = t_1{}^\wedge(\theta) t_2{}^\wedge(\theta)$. In particular, the bounded function corresponding to T^n is $t^\wedge(\theta)^n$. Consequently, if $p \in \mathfrak{I}(T)$, then by (2.3) of § 2,

$$\| (t^\wedge)^n \|_\infty \leqq \| T^n \|_p.$$

Since $\| (t^\wedge)^n \|_\infty = \| t^\wedge \|^n$, we have immediately

$$\| t^\wedge \|_\infty \leqq \liminf_{n \to \infty} \| T^n \|_p{}^{1/n}. \tag{3.1}$$

A little later we shall give a class of multiplier transforms for which the inequality in (3.1) may be replaced by equality.

If T is a bounded operator on l^p, then by the spectrum, $S_p(T)$, of T, we shall mean the class of all complex λ such that $T - \lambda I$ does not have a bounded inverse on l^p.

By the essential range, $R(f)$, of a function $f(\theta)$, we shall mean the class of all λ such that the set $[\theta \mid | f(\theta) - \lambda | < \epsilon]$ has positive Lebesgue measure for every $\epsilon > 0$.

If T is a multiplier transform on l^2, then it is clear that T has a bounded inverse on l^2 if and only if $0 \notin R(t^\wedge)$. Consequently, $S_2(T) = R(t^\wedge)$.

THEOREM 3.1. *If $p \in \mathfrak{I}(T)$, then $S_2(T) \subseteq S_p(T)$.*

Proof. First we note that if T is a multiplier transform on l^p to itself and T^{-1} exists and is bounded, then T^{-1} is a multiplier transform on l^p. For, if $a, b \in l_0$, then

$$T^{-1}(a * b) = T^{-1}((TT^{-1}a) * b) = T^{-1}T((T^{-1}a) * b) = (T^{-1}a) * b.$$

Now, if $\lambda \notin S_p(T)$, then $T_\lambda = T - \lambda I$ has a bounded inverse on l^p, and therefore on l^q, and finally on l^2. But this means $\lambda \notin S_2(T)$. Theorem 3.1 is essentially a special case of a result due to Halberg [14].

THEOREM 3.2. *Let $t^\wedge(\theta)$ be the bounded measurable function corresponding to T. If*[3] *$t^\wedge(\theta +)$ and $t^\wedge(\theta -)$ exist for every $\theta \in [0,1]$, then $S_2(T) = S_p(T)$ for*[4] *$p \in \mathfrak{I}(T)^0$.*

Proof. We first assert that given $\epsilon > 0$, there exists a finite set $\{I_k\}_1{}^n$ of non-overlapping open intervals such that $I - \bigcup_{k=1}^{n} I_k$ $(I = [0,1])$ consists of a finite number of points, and such that

---

[3] It is of course sufficient for $t^\wedge(\theta)$ to have this property after being suitably redefined on a set of measure zero.

[4] $\mathfrak{I}(T)^0$ is the interior of $\mathfrak{I}(T)$.

$$\operatorname*{l.u.b.}_{\theta,\phi\in I_k} | t^\wedge(\theta) - t^\wedge(\phi) | < \epsilon, \qquad k = 1, \cdots, n.$$

To obtain such a set of intervals, let us associate with each point θ of I an open interval J_θ' whose right hand end point is θ such that if $\phi \in J_\theta'$, then $| t^\wedge(\phi) - t^\wedge(\theta -) | < \epsilon/2$, and an open interval J_θ'' whose left hand end point is θ such that if $\phi \in J_\theta''$, then $| t^\wedge(\phi) - t^\wedge(\theta +) | < \epsilon/2$. Finally, let $J_\theta = J_\theta' \cup J_\theta'' \cup \{\theta\}$. For each θ, J_θ is an open interval containing θ. Since I is compact, there exist values $\theta_1, \cdots, \theta_r$ such that $I = \bigcup_{i=1}^{r} (J_{\theta_i} \cap I)$. If we take for the I_k's the open intervals of the decomposition of I formed by the end points of $J_{\theta_1}' \cap I, \cdots, J_{\theta_r}' \cap I$, $J_{\theta_1}'' \cap I, \cdots, J_{\theta_r}'' \cap I$, then these have the desired properties.

Without any loss of generality, it will be enough to show that $0 \notin S_2(T)$ implies $0 \notin S_p(T)$. The result will then follow by Theorem 3.1. Let $m = \text{ess. inf.} | t^\wedge(\theta) |$. If $0 \notin S_2(T)$, then $m > 0$. Given $\epsilon > 0$, let $\{I_k\}_1^n$ be a composition as described above. We choose θ_k in I_k, $k = 1, \cdots, n$, such that $m \leqq | t^\wedge(\theta_k) | \leqq \| t^\wedge \|_\infty$.

If $p_k^\wedge(\theta)$ is the characteristic function of I_k, we have

$$1/t^\wedge(\theta) = \sum_{k=1}^{n} p_k^\wedge(\theta) / \{ t^\wedge(\theta_k) + p_k^\wedge(\theta) [t^\wedge(\theta) - t^\wedge(\theta_k)] \}.$$

Further, if P_k is the operator corresponding to $p_k^\wedge(\theta)$, then since $p_k^\wedge(\theta)$ is of total variation 2, by a theorem of Stečkin [12] (see also [8]), we get $\| P_k \|_p \leqq A(p) < \infty$, where $A(p)$ is independent of k.

We may as well assume there exists an $r \in \mathfrak{S}(T)$ such that $r \neq 2$. For, otherwise the theorem is trivial. We have

$$\| P_k(T - t^\wedge(\theta_k) I \|_r \leqq 2A(r) \| T \|_r \tag{3.2}$$

and

$$\| P_k(T - t^\wedge(\theta_k) I) \|_2 = \| p_k^\wedge(\theta) [t^\wedge(\theta) - t^\wedge(\theta_k)] \|_\infty, \tag{3.3}$$

where I is the identity operator. If p is any number between r and 2, there exists an $0 < \omega < 1$ for which $1/p = (1 - \omega)(1/r) + (1/2)\omega$. By the Riesz-Thorin convexity theorem, (3.2) and (3.3), we get

$$\| P_k(T - t^\wedge(\theta_k) I) \|_p \leqq [2A(r) \| T \|_r]^{1-\omega} \epsilon^\omega.$$

If we choose ϵ so small that

$$[2A(r) \| T \|_r]^{1-\omega} \epsilon^\omega < m,$$

we see that by expanding

$$\{ t^\wedge(\theta_k) + p_k^\wedge(\theta) [t^\wedge(\theta) - t^\wedge(\theta_k)] \}^{-1}$$

into a geometric series, the operator corresponding to this function must be bounded on l^p. Therefore, the operator on l^p corresponding to $1/t^\wedge(\theta)$ must be bounded, and it is clearly the inverse of T.

COROLLARY 3.3. *Under the conditions of Theorem* 3.2,

$$\| t^\wedge(\theta) \|_\infty = \lim_{n\to\infty} \| T^n \|_p^{1/n}.$$

Proof. It is well known that $\| T \|_p^\wedge = \lim \| T^n \|_p^{1/n}$, where $\| T \|_p^\wedge = \sup [|\lambda| \mid \lambda \in S_p(T)]$ (cf. [7], p. 75). Since T is a normal operator on the Hilbert space l^2, we get $\| t^\wedge \|_\infty = \| T \|_2 = \| T \|_2^\wedge$. By Theorem 3.2, we get $\| T \|_2^\wedge = \| T \|_p^\wedge$. Therefore, $\| t^\wedge \|_\infty = \| T \|_p^\wedge$, which gives the result.

This is the promised sharpening of (3.2).

COROLLARY 3.4. *Under the conditions of Theorem* 3.2,

$$S_p(T) = R(t^\wedge).$$

Proof. This follows immediately from the equation

$$S_p(T) = S_2(T) = R(t^\wedge).$$

Corollary 3.4 generalizes results of P. Hartman [2] and G. L. Krabbe [5], [6].

4. The spectrum of multiplier transforms continued. In this section, we shall discuss theorems about multiplier transforms which will give information about their point spectra. We recall that a complex number λ is in the point spectrum of T acting on l^p if $T - \lambda I$ is not one to one; i. e., there exists a non-zero $a \in l^p$ such that $(T - \lambda I)a = 0$. The point spectrum of T is closely connected with the concept of sets of uniqueness and sets of multiplicity for l^p. There are many possibilities for defining a set of uniqueness for l^p. Here we mention only two.

We say that a set $\mathcal{E} \subseteq [0,1]$ *is an ordinary set of uniqueness for* l^p *if* $a \in l^p$ *and*

$$\sum_{-\infty}^{\infty} a(n) e^{2\pi i n\theta} = 0, \qquad \theta \notin \mathcal{E},$$

implies $a = 0$, *where the sum is taken as an ordinary limit.*

If $1 \leqq p \leqq 2$, *we say that* $\mathcal{E}$ *is a mean set of uniqueness for* l^p *if* $a \in l^p$ *and*

$$q - \text{l. i. m.} \sum_{-N}^{N} a(n) e^{2\pi i n\theta} = 0, \qquad \theta \notin \mathcal{E},$$

implies $a = 0$, *where* q — l. i. m. *stands for the limit in the mean of* L^q, *the space of q-summable functions on* $[0,1]$.

An ordinary or mean set of multiplicity for l^p *is a set which is not an ordinary or mean set of uniqueness for* l^p, *respectively.*

When $1 \leqq p \leqq 2$ the point spectrum problem is elementary because of the Hausdorff-Young-Riesz theorem and we have the following result. The proof is left to the reader.

THEOREM 4.1. *If* $p \in \mathfrak{F}(T)$, $1 \leqq p \leqq 2$, *then* λ *is in the point spectrum of* T, *operating on* l^p, *if and only if the set* $[\theta \mid t^\wedge(\theta) = \lambda]$ *is a mean set of multiplicity for* l^p.

We should remark here that no example has yet been given of a mean set of uniqueness for l^p which is of positive measure $(1 < p < 2)$.

When $p > 2$, the situation is more complex. Let

$$\mathcal{E}_{\epsilon\lambda} = [\theta \mid \mid t^\wedge(\theta) - \lambda \mid < \epsilon]$$

and let

$$\mathcal{E}_\lambda = \bigcap_{\epsilon > 0} \bar{\mathcal{E}}_{\epsilon\lambda}.$$

THEOREM 4.2. *Let*[3] $p \in \mathfrak{F}(T)^0$ *and let* $t^\wedge(\theta)$ *satisfy the assumptions of Theorem* 3.2. *If* $a \in l^p$ *and* $(T - \lambda I)a = 0$, *then*

$$\sum_{-\infty}^{\infty} a(n) e^{2\pi i n\theta} = 0, \qquad \theta \notin \mathcal{E}_\lambda.$$

Proof. Without any loss of generality, we may suppose $\lambda = 0$. Let

$$a_h(n) = \begin{cases} a(n) \sin 2\pi n h / 2\pi n h, & n \neq 0 \\ 1. & n = 0. \end{cases}$$

Further, let

$$A(\theta) = a(0)\theta + \sum_{-\infty}^{\infty}{}' (a(n)/2\pi i n) e^{2\pi i n\theta},$$

this series converging absolutely. Then

$$A_h(\theta) = [A(\theta + h) - A(\theta - h)]/2h = \sum_{-\infty}^{\infty} a_h(n) e^{2\pi i n\theta}, \qquad |h| > 0.$$

Let $I = [u, v]$ be any closed interval in the complement of $\mathcal{E}_0$. By the proof of Theorem 3.2, it is easy to see that

$$p^\wedge(\theta) = \begin{cases} 1/t^\wedge(\theta) & \theta \in I \\ 0 & \theta \notin I \end{cases}$$

gives rise to a bounded multiplier transform P on $\mathfrak{F}(T)$. Therefore, since Ta_h and Pe are in l^2, we have, by Parseval's equality,

$$(Ta_h, Pe) = \int_0^1 A_h(\theta) t^\wedge(\theta) p^\wedge(\theta)\, d\theta = \int_\mu^\nu A_h(\theta)\, d\theta.$$

Now, $a_h \to a$, and therefore $Ta_h \to Ta$ in l^p. Hence,

$$\lim_{h\to 0}(Ta_h, Pe) = \lim_{h\to 0}\int_\mu^\nu A_h(\theta)\, d\theta = A(\nu) - A(\mu) = 0.$$

Consequently, $A(\theta)$ is constant on each interval of the complement of $\mathcal{E}_0$ and this in turn implies that $\sum a(n) e^{2\pi in\theta} = 0$ on each such interval (see [13], p. 270).

The converse of Theorem 4.2 can be proved, provided more assumptions are put on $t^\wedge(\theta)$. This will be shown in the next theorem. We first need a definition.

A function $f(\theta)$, $\mu \leqq \theta \leqq \nu$, is said to be of bounded β-variation,[5] $\beta > 0$, if

$$V_\beta[f] = \sup[\sum_{k=0}^{n} | f(\theta_{k+1}) - f(\theta_k) |^\beta]^{1/\beta} < \infty,$$

where the supremum is taken over all finite decompositions of the form $\mu = \theta_0 < \theta_1 < \cdots < \theta_{n+1} = \nu$.

The reader may easily verify that for functions of bounded β-variation, $f(\theta+)$ and $f(\theta-)$ exist. Therefore, these functions can have at most a countable number of singularities and they satisfy the conditions of Theorem 3.2.

THEOREM 4.3. *Let $t^\wedge(\theta)$ be of bounded β-variation for some $\beta > 0$. If $p \in \mathfrak{S}(T)$, $2 < p < \infty$, $a \in l^p$ and*

$$\sum_{-\infty}^{\infty} a(n) e^{2\pi in\theta} = 0, \qquad \theta \notin \mathcal{E}_\lambda,$$

then

$$(T - \lambda I)^m a = 0,$$

for m an integer and $m \geqq \beta(p-2)/2p$.

Proof. Without any loss of generality, we may assume $\lambda = 0$. Since $\mathcal{E}_0$ is a closed set, its complement is the union of at most a countable set of open intervals, $\{I_k\}$. As in Theorem 4.2, let

$$A(\theta) = a(0)\theta + \sum_{-\infty}^{\infty} (a(n)/2\pi in) e^{2\pi in\theta},$$

and

$$A_h(\theta) = [A(\theta + h) - A(\theta - h)]/2h = \sum_{-\infty}^{\infty} a_h(n) e^{2\pi in\theta}, \quad h > 0,$$

---

[5] For a further discussion of β-variation and multiplier transforms see [3].

where, as before, $a_h(n) = a(n)s_h(n)$, where $s_h(0) = 1$ and $s_h(n) = \sin 2\pi nh/2\pi nh$ if $n \neq 0$. If $I_k = (\mu_k, \nu_k)$ and $2h < (\nu_k - \mu_k)$, then $A_h(\theta) = 0$ for $\theta \in [\mu_k + h, \nu_k - h]$.

As usual, let e be the identity element of l^p and $e_n(m) = e(m+n)$. We have

$$
\begin{aligned}
(a_h, T^m e_n) &= \int_0^1 A_h(\theta)\, t^\wedge(\theta)^m e^{-2\pi i n\theta}\, d\theta \\
&= \sum_{k=1}^{N} \int_{I_k} A_h(\theta)\, t^\wedge(\theta)^m e^{-2\pi i n\theta}\, d\theta \qquad (4.1)\\
&\quad + \sum_{k=N+1}^{\infty} \int_{I_k} A_h(\theta)\, t^\wedge(\theta)\, e^{-2\pi i n\theta}\, d\theta.
\end{aligned}
$$

Since $a_h \to a$ in l^p and T^m is bounded, it follows that

$$
\lim_{h\to 0} (a_h, T^m e_n) = (a, T^m e_n) = T^m a(n). \qquad (4.2)
$$

Further, we claim that

$$
\lim_{h\to 0} \int_{I_k} A_h(\theta)\, t^\wedge(\theta)^m e^{-2\pi i n\theta}\, d\theta = 0
$$

for any k. For,

$$
\Big[\int_{I_k} | A_h(\theta)\, t^\wedge(\theta)^m |\, d\theta\Big]^2 \leq \int_0^1 | A_h(\theta)|^2\, d\theta \int_{H_k} | t^\wedge(\theta)|^{2m}\, d\theta,
$$

where $H_k = (\mu_k, \mu_k + h] \cup [\nu_k - h, \nu_k)$ for $2h < |I_k|$ $(|I_k| = \nu_k - \mu_k)$. Also,

$$
\int_0^1 | A_h(\theta)|^2\, d\theta = \sum_{-\infty}^{\infty} | a_h(n)|^2 \leq \Big[\sum_{-\infty}^{\infty} | a(n)|^p\Big]^{2/p} \Big[\sum_{-\infty}^{\infty} | s_h(n)|^{2p/(p-2)}\Big]^{(p-2)/p},
$$

and since $p/(p-2) > 1$, we get, by an easy estimation,

$$
\sum_{-\infty}^{\infty} | s_h(n)|^{2p/(p-2)} = O(1/h).
$$

Consequently,

$$
\int_0^1 | A_h(\theta)|^2\, d\theta = O(h^{(2-p)/p}).
$$

Since

$$
\int_{H_k} | t^\wedge(\theta)|^{2m}\, d\theta = O(h),
$$

we have

$$
\int_{I_k} A_h(\theta)\, t^\wedge(\theta)^m e^{-2\pi i n\theta}\, d\theta = O(h^{2/p}) \to 0 \text{ as } h \to 0.
$$

Therefore, the limit of the first sum in (4.1) is zero. If we can show that the second sum in this equation is small for suitable values of m, provided

N is sufficiently large independently of h, then this combined with equation (4.2) will complete the proof of the theorem.

We have

$$\sum_{N+1}^{\infty}\int_{I_k} A_h(\theta)t^\wedge(\theta)^m e^{-2\pi in\theta}\,d\theta=\sum_{1}^{\infty}\int_{J_k} A_h(\theta)t^\wedge(\theta)^m e^{-2\pi in\theta}\,d\theta,$$

where J_k is one of the intervals $(\mu_r,\mu_r+h]$ or $[\nu_r-h,\nu_r)$ in case $2h<|I_r|$, or is I_r in case $2h\geqq|I_r|$, $r>N$. Since the J_k are mutually disjoint, we get

$$\begin{aligned}\Big[\sum_{1}^{\infty}\int_{J_k} A_h(\theta)t^\wedge(\theta)^m\,|\,d\theta\Big]^2&=\Big[\int_{U_N}|A_h(\theta)t^\wedge(\theta)^m|\,d\theta\Big]^2\\&\leqq\int_0^1|A_h(\theta)|^2\,d\theta\int_{U_N}|t^\wedge(\theta)|^{2m}\,d\theta\\&\leqq O(h^{2/p-1})\Big[\int_{U_N}|t^\wedge(\theta)|^{2m\alpha}\Big]^{1/\alpha}|U_N|^{1/\beta},\end{aligned}\tag{4.3}$$

where $U_N=\cup J_k$; $|U_N|$ is the Lebesgue measure of U_N, $\alpha>1$ and $1/\alpha+1/\beta=1$. If $J_k=(\mu_r,\mu_r+h]$, then $t^\wedge(\mu_r-)=0$; if $J_k=[\nu_r-h,\nu_r)$, then $t^\wedge(\nu_r+)=0$; if $J_k=(\mu_r,\nu_r)$, then $t^\wedge(\mu_r-)=t^\wedge(\nu_r+)=0$. We shall designate the appropriate end point of J_k by θ_k and we have $t^\wedge(\theta_k\pm)=0$, with the correct sign chosen, depending on the end point. Therefore,

$$\begin{aligned}\int_{U_N}|t^\wedge(\theta)|^{2m\alpha}\,d\theta&=\sum_{1}^{\infty}\int_{J_k}|t^\wedge(\theta)|^{2m\alpha}\,d\theta\\&=\sum_{1}^{\infty}\int_{J_k}|t^\wedge(\theta)-t^\wedge(\theta_k\pm)|^{2m\alpha}\,d\theta.\end{aligned}\tag{4.4}$$

Now, in J_k, the supremum of $t^\wedge(\theta)$ exists and is of the form $t^\wedge(\theta_k'+)$ or $t^\wedge(\theta_k'-)$, where $\theta_k'\in\bar{J}_k$, the closure of J_k. Therefore,

$$\begin{aligned}\sum_{1}^{\infty}\int_{J_k}|t^\wedge(\theta)-t^\wedge(\theta_k\pm)|^{2m\alpha}\,d\theta&\leqq h\sum_{1}^{\infty}|t^\wedge(\theta_k'\pm)-t^\wedge(\theta_k\pm)|^{2m\alpha}\\&\leqq hV_{2m\alpha}[t^\wedge]^{2m\alpha}.\end{aligned}\tag{4.5}$$

If we choose $m\geqq\beta/2\alpha$, then $V_{2m\alpha}[t^\wedge]$ is, by hypothesis, finite. If we take $\alpha=p/(p-2)$, then from (4.3), (4.4) and (4.5) we get

$$\Big[\sum_{N+1}^{\infty}\int_{I_k} A_h(\theta)t^\wedge(\theta)e^{-2\pi in\theta}\,d\theta\Big]^2=O(|U_N|^{2/p}).$$

Since $|U_N|\to0$ as $N\to\infty$, the left side goes to zero independently of h. This completes the proof of our theorem.

Remark. The restriction $p>2$ in Theorem 4.3 is really no essential restriction. While Theorem 4.3 is true for $p\leqq2$, Theorem 4.1 gives a slightly stronger result. Notice for the case $\beta = 2p/(p-2)$, Theorem 4.3 is a direct converse of Theorem 4.2.

The method of proof we have used in this theorem is an extension of a method used by H. Pollard in [10], and C. Herz [4].

Notice that if $t^\wedge(\theta)$ satisfies the conditions of Theorem 3.2 and λ is in the point spectrum of T acting on l^p, $p \in \mathfrak{Z}(T)^0$, then $\mathcal{E}_\lambda$ is an ordinary set of multiplicity for l^p. Conversely, if $t^\wedge(\theta)$ satisfies the condition of Theorem 4.3 and $\mathcal{E}_\lambda$ is an ordinary set of multiplicity for l^p, $p \in \mathfrak{Z}(T)$ $(1 < p < \infty)$, then λ is in the point spectrum of T.

Remark. For continuous functions $t^\wedge(\theta)$, the set $\mathcal{E}_\lambda$ coincides with the set of θ where $t^\wedge(\theta) = \lambda$. The same is true for functions of bounded β-variation if they they are normalized by the condition that $t^\wedge(\theta) = \lambda$ if either $t^\wedge(\theta+) = \lambda$ or $t^\wedge(\theta-) = \lambda$. More generally, if $t^\wedge(\theta)$ is any function such that $t^\wedge(\theta+)$ and $t^\wedge(\theta-)$ exist, then for fixed λ, $t^\wedge(\theta)$ may be normalized so that $\mathcal{E}_\lambda$ is the set where $t^\wedge(\theta) = \lambda$.

Suppose now that $t^\wedge(\theta)$ is a function of bounded variation on $[0,1]$. In [2], P. Hartman poses the following question: Is λ an eigenvalue for T acting on l^p if and only if $[\theta \mid t^\wedge(\theta) = \lambda]$ is of positive Lebesgue measure? The following considerations show that the necessity part of this question must have a negative answer for $p > 2$.

In [11], R. Salem exhibites a perfect set $\mathcal{E}$ of Lebesgue measure zero and a continuous singular measure $d\mu$ with spectrum $\mathcal{E}$ so that

$$a(n) = \int_0^1 e^{-2\pi i n\theta}\, d\mu(\theta)$$

belongs to l^q for every $q > 2$. Clearly, it is possible to construct a continuous function $t^\wedge(\theta)$ of bounded variation which vanishes on $\mathcal{E}$, and is different from zero on the complement of $\mathcal{E}$. We have

$$Ta(n) = t * a(n) = \int_0^1 e^{-2\pi i n\theta}\, t^\wedge(\theta)\, d\mu(\theta) = 0,$$

which gives our result.

5. Two theorems connected with spectral synthesis in l^∞.

Let $a \in l^\infty$ and

$$B(\theta) = a(0)\theta^2/2 + \sum_{-\infty}^{\infty}{}' \,(a(n)/-4\pi n^2)\, e^{2\pi i n\theta}.$$

If $t \in l^1$, then H. Pollard [10] has shown[6] that $t * a = 0$ only if $B(\theta)$ is linear on each interval contiguous to the set of zeros of $t^\wedge(\theta)$. It is not known whether the converse statement is true or false. Here we shall prove the converse statement for certain classes of sequences in l^1. We refer the reader to Pollard's paper for a complete discussion of the problem of spectral synthesis.

---

[6] Actually, Pollard is working on the group of real numbers. However, his methods also work here without essential modication.

Let $f(\theta)$ be a function defined on $[0,1]$ and I any subinterval of this set with end points μ and ν. We shall write $f(I)=f(\nu)-f(\mu)$ and $|I|=\nu-\mu$. Let $\{I_k\}$ be a set of non-overlapping intervals each of which is contained in $[0,1]$. *We shall say that* $f(\theta)$ *is* β*-absolutely continuous if for any* $\epsilon>0$ *there exists a* $\delta>0$ *so that* $\sum|I_k|<\delta$ *implies* $\sum|f(I_k)|^\beta<\epsilon$.

THEOREM 5.1. *Let* $t\in l^1$, $t^\wedge(\theta)$ *its Fourier series,* T *the corresponding multiplier transform and* $a\in l^\infty$. *If* $B(\theta)$ *is linear on each open interval contiguous to the set of zeros of* $t^\wedge(\theta)$ *and* $t^\wedge(\theta)$ *is* β*-absolutely continuous, then*

$$T^m a=0,$$

where m *is an integer and* $m\geqq\beta/2$.

The proof of this theorem is similar to the proof of Theorem 4.3 and we leave the details to the reader.

Another theorem whose proof does not seem to follow from the considerations of the proof of Theorem 4.3 concerns those functions $t^\wedge(\theta)$ which belong to an integral Lipschitz class. Although the proof of our theorem is quite easy, it does not seem to have been recorded. We say that $f(\theta)\in \mathrm{Lip}(\alpha,p)$ if there exists a constant A such that for every h,

$$\left[\int_0^1|f(\theta+h)-f(\theta)|^p\,d\theta\right]^{1/p}<A|h|^\alpha.$$

We need the following theorem which is essentially due to S. Bernstein. A proof may be found in Zygmund [13], p. 135.

BERNSTEIN'S THEOREM. *If*

$$\int_0^1|t^\wedge(\theta+h)-t^\wedge(\theta)|^2\,d\theta<A|h|^{2\alpha},$$

$2\alpha>1$, *then there exists a constant* B, *independent of* A *and* α *such that*

$$\sum_{2^{n-1}<|k|\leqq 2^n}|t(k)|<AB\,2^{-n(1/2-\alpha)}, \tag{5.1}$$

and consequently,

$$\sum_{-\infty}^{\infty}|t(n)|<|t(0)|+AB\sum_{-\infty}^{\infty}{}'\,2^{-n(1/2-\alpha)}. \tag{5.2}$$

THEOREM 5.2. *Let* $t \in l^1$, $t^\wedge \in \mathrm{Lip}(\alpha, 2)$, $\alpha > \frac{1}{2}$, *and* $a \in l^\infty$. *If* $B(\theta)$ *is linear on each open interval contiguous to the set of zeros of* $t^\wedge(\theta)$, *then* $Ta = t * a = 0$.

Proof. Consider the operator defined on the complex z-plane by the conditions

$$C_\rho z = \begin{cases} \rho z/|z| & \text{if } |z| \geqq \rho \\ z & \text{if } |z| < \rho \end{cases} \qquad (\rho > 0).$$

The operator C_ρ has been called by Beurling [1] a circular contraction. If we set $t^\wedge_\rho = C_\rho t^\wedge$, it is quite obvious that

$$(5.3) \qquad \int_0^1 |t^\wedge_\rho(\theta + h) - t^\wedge_\rho(\theta)|^2 \, d\theta \leqq \int_0^1 |t^\wedge(\theta + h) - t^\wedge(\theta)|^2 \, d\theta.$$

From (5.3), the hypothesis of the theorem and Bernstein's theorem it follows that t and t_ρ belong to l^1.

Set

$$\begin{aligned} B_h(\theta) &= [B(\theta + 2h) - 2B(\theta) + B(\theta - 2h)]/4h \\ &= \sum_{-\infty}^{\infty} b_h(n) e^{2\pi i n \theta}, \qquad |h| > 0, \end{aligned}$$

where $b_h(0) = a(0)$, $b_h(n) = a(n)(\sin 2\pi n h / 2\pi n h)^2$ if $n \neq 0$. For fixed ρ, it follows from the continuity of $t^\wedge(\theta)$ that if h is sufficiently small, then $B_h(\theta) = 0$ everywhere that $[t^\wedge(\theta) - t^\wedge_\rho(\theta)] \neq 0$. Therefore, by the Parseval theorem, we get

$$(b_h, [T - T_\rho] e_n) = \int_0^1 B_h(\theta) [t^\wedge(\theta) - t^\wedge_\rho(\theta)] e^{-2\pi i n \theta} \, d\theta = 0,$$

where $e_n(m) = 0$ if $n + m \neq 0$, $e_n(-n) = 1$. Now, for every m,

$$|b_h(m)| \leqq |a(m)| \text{ and } b_h(m) \to a(m) \text{ as } h \to 0.$$

Therefore,

$$\begin{aligned} (a, [T - T_\rho] e_n) &= \lim_{h \to 0} \sum_{m=-\infty}^{\infty} b_h(m) [T - T_\rho] e_n(-m) \\ &= \lim_{h \to 0} (b_h, [T - T_\rho] e_n) = 0. \end{aligned}$$

This means that

$$(5.4) \qquad Ta = T_\rho a$$

Clearly, for every m, $t_\rho(m) \to 0$ as $\rho \to 0$. Therefore, from (5.3), the hypothesis of Theorem 5.2 and formulas (5.1) and (5.2) of Bernstein's theorem, we get

$$\| T_\rho \|_1 = \sum_{-\infty}^{\infty} |t_\rho(m)| \to 0 \quad \text{as } \rho \to 0.$$

This, combined with (5.4), gives $Ta = 0$, which completes the proof of the theorem.

WASHINGTON UNIVERSITY.

REFERENCES.

[1] A. Beurling, " On the spectral synthesis of bounded functions," *Acta Mathematica*, vol. 81 (1948), pp. 1-14.

[2] P. Hartman, " On Laurent operators on l_p," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 45-48.

[3] I. I. Hirschman, Jr., " On multiplier transformations " (to be published).

[4] C. S. Herz, "A note on the span of translations in L^p," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 724-727.

[5] G. L. Krabbe, "Abelian rings and spectra of operators on l_p," *ibid.*, vol. 7 (1956), pp. 783-790.

[6] ———, " Spectral isomorphisms for some rings of infinite matrices on a Banach space," *American Journal of Mathematics*, vol. 78 (1956), pp. 42-50.

[7] H. Loomis, *An introduction to abstract harmonic analysis*, Toronto-New York-London, 1953.

[8] J. Marcinkiewicz, " Sur les multiplicateurs des series de Fourier," *Studia Mathematica*, vol. 8 (1939), pp. 78-91.

[9] H. Pollard, " The closure of translations in L^p," *Proceedings of the American Mathematical Society*, vol. 2 (1951), pp. 100-104.

[10] ———, " The harmonic analysis of bounded functions," *Duke Mathematical Journal*, vol. 20 (1953), pp. 499-512.

[11] R. Salem, " On singular monotonic functions of the Cantor type," *Journal of Mathematics and Physics*, vol. 21 (1942), pp. 69-82.

[12] S. B. Stečkin, " On bilinear forms," *Doklady Akademii Nauk SSSR*, N. S., vol. 71 (1950), pp. 237-240.

[13] A. Zygmund, *Trigonometrical series*, Warsaw-Lwow, 1935.

[14] C. J. A. Halberg, Jr., " The spectra of bounded linear operators on sequence spaces," *Proceedings of tht American Mathematical Society*, vol. 8 (1957), pp. 728-732.

THE INTEGRAL REPRESENTATIONS OF QUADRATIC FORMS OVER LOCAL FIELDS.*

By O. T. O'Meara.

Dedicated to Artin on his sixtieth birthday.

A quadratic form q which is obtained from a given form Q by a linear substitution of any number of new variables is called a representation of Q. As a special case we have the notion of equivalence of forms, the linear substitution then being a change of variables that can be inverted over the basic coefficient ring. One of the problems of interest in the arithmetic theory of forms is to determine all the representations of a given quadratic form. Using p-adic theory, Hasse [4] solved this problem over the rational numbers. An account of the rational and p-adic theory can be found in the book by Jones [6]. In both these cases the basic rings are fields; much less is known about integral representation, but the special problem of integral equivalence has been solved locally, and complete solutions can be found by consulting the works of Minkowski, Jones, Pall and O'Meara that are listed at the end of this paper. Conditions for the p-adic integral representation of one unimodular form by another are given by Jones at the odd primes [6]. It is our intention here to give necessary and sufficient conditions that will determine the integral representations of an arbitrary quadratic form over any local field in which 2 is either a unit or a prime.

Complete conditions for field representation are known for local fields, and we make this the basis of our discussion. Our criteria for the integral representation of one form by another will be in terms of the field representations of forms derived from certain canonical decompositions of the given forms.

I. Basic Concepts.

Summary. Our basic field F will be a local field [1] with ring of integers $\mathfrak{o}$ and prime ideal $\pi\mathfrak{o}$. We assume that $\operatorname{char} F \neq 2$, and that the residue class field $\mathfrak{o}/(\pi\mathfrak{o})$ is finite. We denote the multiplicative group of F by F^*,

---

* Received January 17, 1958.

and the group of units by $\mathfrak{u}$. Later on, we make special assumptions about the behaviour of 2 in F.

We shall consider finite dimensional vector spaces $U, V, W, \cdots$ over F. If V is provided with a scalar product $x \cdot y \in F$, we call it a quadratic space. For an $\alpha \in F^*$, we shall write $\alpha \circ V$ to mean the new quadratic space given by putting $x \circ y = \alpha(x \cdot y)$ on the old vector space V. We shall use $\bigoplus_1^p V_\lambda$ to denote the orthogonal (direct) sum of the quadratic spaces V_λ $(1 \leqq \lambda \leqq p)$. The radical of V will be written rad V. A non-degenerate space is one in which rad $V = 0$. The quadratic space V has a radical decomposition $V = U \oplus \text{rad } V$ in which U is non-degenerate. Any non-degenerate subspace U of a non-degenerate space V is a component of V, i. e. there is a non-degenerate subspace W such that $V = U \oplus W$. Moreover, W is then uniquely determined as $U^\perp$, and $U^{\perp\perp} = U$. An isotropic vector is a non-zero vector x for which $x^2 = 0$. For subsets S_1, S_2 of V, we write

$$S_1 \cdot S_2 = \{s_1 \cdot s_2 \mid s_1 \in S_1, s_2 \in S_2\},$$

$$S_1^2 = \{s_1^2 \mid s_1 \in S_1\}.$$

For further details on quadratic spaces, the reader is referred to *Geometric Algebra*, Ch. III.

By a lattice L in V we mean an $\mathfrak{o}$-module in the vector space V with the following property: the coordinates of the elements of L have bounded denominators in any basis for V. If this property holds for a single basis it must hold for all bases. The set 0 is a lattice in the space $V = 0$. Any $\mathfrak{o}$-module in L is again a lattice in V. The vector space spanned by L is the set FL. If L is the direct sum $\sum L_\lambda$, then FL is the direct sum $\sum FL_\lambda$. If L has a basis $\langle x \rangle$, then $\langle x \rangle$ is also a basis for FL. If FL has a basis $\langle y \rangle$, there is a basis $\langle z \rangle$ for $L = \sum \mathfrak{o} z_\lambda$ such that $Fy_1 + \cdots + Fy_i = Fz_1 + \cdots + Fz_i$ holds when $1 \leqq i \leqq \dim FL$. We can therefore speak of the dimension $\dim L$. An $\mathfrak{o}$-linear map of l into L can be extended to an F-linear map of Fl into FL. If the original map is an isomorphism, so is the extended one. In particular, an isomorphism preserves dimension. Given any non-zero x in FL, there is an $\alpha \in F$ such that $\alpha x \in L$, $\alpha\pi^{-1}x \notin L$. We put $\alpha L = \{\alpha x \mid x \in L\}$.

Now consider the lattice L as a subset of the quadratic space V. For an $\alpha \in F^*$ we shall write $\alpha \circ L$ to mean the same set L, but now as part of the quadratic space $\alpha \circ V$. We define L as the orthogonal sum $\bigoplus_1^p L_\lambda$ if (i) L is the direct sum of the L_λ, (ii) the L_λ are mutually orthogonal. Note that

$FL = \oplus FL_\lambda$ if $L = \oplus L_\lambda$. We say that a sublattice K is a component of L if there is a sublattice J such that $L = K \oplus J$. We define the radical as the lattice $\operatorname{rad} L = \{x \in L \mid x \cdot L = 0\}$. We then have

$$F \operatorname{rad} L = \operatorname{rad} FL, \qquad \operatorname{rad} L = L \cap \operatorname{rad} FL.$$

We call L degenerate if $\operatorname{rad} L \neq 0$. If $L = J \oplus K$, then L is non-degenerate if and only if J and K are. If J is non-degenerate, then K is unique and equal to $J^\perp$. For any L we have $L = K \oplus \operatorname{rad} L$.

From now until the end of this section we assume that V and L are non-zero so that they possess bases, the first over F the second over $\mathfrak{o}$. Associated with any basis $\langle x \rangle$ of the quadratic space V is the quadratic form

$$q(\alpha_1, \cdots, \alpha_n) = (\alpha_1 x_1 + \cdots + \alpha_n x_n)^2,$$

and varying $\langle x \rangle$ produces the entire fractional class of q. By $d(V)$ we mean the well-defined image of $\det(x_i \cdot x_j)$ in $0 \cup F^*/(F^*)^2$. We shall sometimes mean by $d(V)$ a particular representative of $d(V)$, for example $\det(x_i \cdot x_j)$. In the same way we can associate a quadratic form q with a basis of L, and varying $\langle x \rangle$ produces the entire unimodular class of q. Moreover, every unimodular class can be obtained from some lattice in such a way. We call $(x_i \cdot x_j)$ the matrix associated with $\langle x \rangle$ and write $L \cong (x_i \cdot x_j)$. By $d(L)$ we mean the well-defined image of $\det(x_i \cdot x_j)$ in $0 \cup F^*/\mathfrak{u}^2$. We shall sometimes denote by $d(L)$ a particular representative $\det(x_i \cdot x_j)$. Note that $d(FL) = d(FK)$ if $d(L) = d(K)$. We see that

$$d(\oplus V_\lambda) = \prod d(V_\lambda), \qquad d(\oplus L_\lambda) = \prod d(L_\lambda);$$

we also have $\operatorname{rad} V \neq 0$ if and only if $d(V) = 0$, and the same for L.

Representations. Let V, V' be two quadratic spaces. We say that V' represents V, and write it $V \to V'$, if there is an F-linear mapping ϕ of V into V' such that $(\phi x)^2 = x^2$ for all $x \in V$. In virtue of the equation $x \cdot y = \frac{1}{2}\{(x+y)^2 - x^2 - y^2\}$ we deduce that $\phi x \cdot \phi y = x \cdot y$. We call ϕ an isometry if it is one-one and onto, and we write $V \cong V'$. If $\phi_1 : (V_1 \to V_1')$ and $\phi_2 : (V_2 \to V_2')$ are representations, there is a unique extension of ϕ_1, ϕ_2 to a representation

$$\phi : (V_1 \oplus V_2 \to V_1' \oplus V_2').$$

If ϕ_1, ϕ_2 are isometries, so is ϕ. Consider radical decompositions

$$V = U \oplus \operatorname{rad} V, \qquad V' = U' \oplus \operatorname{rad} V',$$

and define $\psi : (U \to U')$ by

$$\phi x = \psi x + z, \qquad \psi x \in U',\ z \in \operatorname{rad} V'.$$

Then ψ is a representation. Since U is non-degenerate, ψ can have no kernel so it is actually an isometry of U into U'. We have therefore proved that

$$U \oplus \operatorname{rad} V \rightarrow U' \oplus \operatorname{rad} V' \Leftrightarrow U \rightarrow U'.$$

The same discussion holds for lattices, except for the fact that we use an $\mathfrak{o}$-linear map ϕ to define a representation of L into L'. All the previous results for spaces carry over to lattices, including the extension of a representation to an orthogonal sum, and

$$K \oplus \operatorname{rad} L \rightarrow K' \oplus \operatorname{rad} L' \Leftrightarrow K \rightarrow K'.$$

We also see that a representation $\phi: (L \rightarrow L')$ can be extended uniquely to a representation $FL \rightarrow FL'$; if ϕ is an isometry, so is its extension.

Now let V, V' be non-zero so that they have bases $\langle x \rangle$, $\langle x' \rangle$, with associated quadratic forms q, q'. Consider the representation $\phi: (V \rightarrow V')$. If we write $\phi x_i = \sum t_{\lambda i} x_\lambda'$, we see that

$$x_i \cdot x_j = \phi x_i \cdot \phi x_j = \sum \sum t_{\lambda i} (x_\lambda' \cdot x_\mu') t_{\mu j}$$

and hence the matrix $(x_i' \cdot x_j')$ represents the matrix $(x_i \cdot x_j)$. Thus q' represents q. Reversing the argument shows that $V \rightarrow V'$ if $q \rightarrow q'$. Hence the problem of representation of forms is equivalent to the problem of representation of quadratic spaces. In the very same way we see that the integral representation problem for forms is equivalent to the representation problem for lattices. As for ourselves, we prefer the lattice approach to representation theory because of the geometrical insight it provides. We are not going to refer to the quadratic forms again in this paper.

Now consider the radical decompositions

$$V = U \oplus \operatorname{rad} V, \qquad V' = U' \oplus \operatorname{rad} V'.$$

In practice, one has constructive methods for determining such decompositions. And $V \rightarrow V'$ if and only if $U \rightarrow U'$. The same applies to lattices. We shall therefore assume from now on that all *given lattices or spaces are without radical.* Under this assumption, every representation is an isometry into. Note that lattices or spaces that arise from the given ones, for example by inclusion, may be degenerate. We also assume that all *given* lattices are non-zero, although zero lattices will be allowed to turn up in discussions. We make no such assumption about our spaces which can be zero or non-zero.

PROPOSITION 1. *$U \rightarrow V$ if and only if a replica of U is a component of V.*

PROPOSITION 2. *If $V_1 \oplus U_1 \rightarrow V_2 \oplus U_2$ with $V_2 \rightarrow V_1$, then $U_1 \rightarrow U_2$.*

Proof. We have $V_2 \oplus V^* \oplus U_1 \oplus W^* \cong V_2 \oplus U_2$ by the last proposition. Hence $V^* \oplus U_1 \oplus W^* \cong U_2$ by Witt's theorem. Hence $U_1 \to U_2$. q. e. d.

DEFINITION. *If* $U \to V$, *define* (V/U) *so that* $V \cong U \oplus (V/U)$. *Otherwise, put* $(V/U) = \emptyset$. *Define* $L/l = FL/Fl$.

By Witt's theorem, V/U is well-defined. We also have

$$(1) \qquad (V \oplus W)/(U \oplus W) \cong V/U, \qquad (L \oplus J)/(K \oplus J) \cong L/K$$

It is easily seen that $\alpha \circ (FL) = F(\alpha \circ L)$, $\alpha \circ (V/U) \cong (\alpha \circ V)/(\alpha \circ U)$, $\alpha \circ (L/l) \cong (\alpha \circ L)/(\alpha \circ l)$.

Proposition 1 reduces the problem of representation of spaces to one of finding spaces with given Hasse invariants. The latter question has been solved over local fields and we shall make use of this fact in an indirect way, by expressing criteria for lattice representation in the form $U \to V$ where U, V are derived from the given lattices. The following proposition, whose proof is immediate, is a poor relative of Proposition 1.

PROPOSITION 3. $l \to L$ *if and only if* L *contains a replica of* l.

Maximal lattices. Let $\mathfrak{p}$ be a non-zero ideal in F and let L be any lattice in the quadratic space V. We use $N(L)$ for the norm ideal generated by $x^2, x \in L$. Call L integral if $N(L) \subseteq \mathfrak{o}$. We say that L is $\mathfrak{p}$-maximal in V if (i) $N(L) \subseteq \mathfrak{p}$, (ii) $N(K) \supset \mathfrak{p}$ whenever $K \supset L$. Let l be any lattice in V with $N(l) \subseteq \mathfrak{p}$. By taking a suitably scaled orthogonal basis for $(Fl)^{\perp}$, it is easy to find another lattice $l' \supseteq l$ with $N(l') \subseteq \mathfrak{p}$ and $\dim l' = \dim V$. In particular, every maximal lattice in a space has the dimension of the space itself. We now prove that every lattice l of norm $N(l) \subseteq \mathfrak{p}$ is contained in a $\mathfrak{p}$-maximal lattice. We can assume that $\dim l = \dim V$. By replacing V by $\alpha \circ V$ if necessary, we can take $\mathfrak{p} \subseteq 2\mathfrak{o}$. Take a strictly increasing sequence $l \subset l_1 \subset l_2 \subset \cdots$, in which all lattices have norm in $\mathfrak{p}$. Then $|d(l)| < |d(l_1)| < |d(l_2)| < \cdots$. Now $l_\lambda \cdot l_\lambda \subseteq \mathfrak{o}$ since $N(l_\lambda) \subseteq 2\mathfrak{o}$. Hence $d(l_\lambda) \subseteq \mathfrak{o}$. Hence the sequence terminates. Hence l is contained in a $\mathfrak{p}$-maximal lattices. Eichler [3] uses maximal lattices in a slightly different sense, but the following proposition follows immediately from his results.

PROPOSITION 4. *Two* $\mathfrak{p}$*-maximal lattices in the same quadratic space are isometric.*

Proof. We can suppose that $\mathfrak{p} = \mathfrak{o}$. First let the space V be anisotropic. By Theorem 9.4 of [3], we see that

$$\{x \in V \mid x^2 \in \mathfrak{o}\}$$

is a lattice, and it clearly contains every integral lattice in V. Thus there is only one $\mathfrak{o}$-maximal lattice and there is nothing to prove.

Now let V be isotropic. First we prove that any $\mathfrak{o}$-maximal L has norm $\mathfrak{o}$. Let x_0 be an isotropic vector in L such that $x_0 \notin \pi L$. Suppose, if possible, that $x_0 \cdot L \subseteq \frac{\pi}{2}\mathfrak{o}$. Then

$$J = \{ (\alpha/\pi)x_0 + y \mid \alpha \in \mathfrak{o}, y \in L\}$$

is also a lattice, $N(J) \subseteq \mathfrak{o}$, and $J \supset L$, which denies the maximality of L. Hence $x_0 \cdot L = \frac{1}{2}\mathfrak{o}$. Let $y_0 \in L$ be such that $x_0 \cdot y_0 = \frac{1}{2}$. If $y_0{}^2$ is not a unit, then $(x_0 + y_0)^2$ is a unit. Hence $N(L) = \mathfrak{o}$. This proves the contention. If K is another $\mathfrak{o}$-maximal lattice in V, we have $N(L) = N(K) = \mathfrak{o}$. But L, K are maximal in the sense of Eichler and their norms are the same, hence $L \cong K$ by Theorem 9.6 of [3].

Jordan forms. We call l π^i-modular, or simply modular, if

$$x \in l, x \notin \pi l \Longrightarrow x \cdot l = \pi^i \mathfrak{o};$$

we call a modular l proper if $N(l) = l \cdot l$, we call it improper if $N(l) \subset l \cdot l$. Improper lattices do not occur when 2 is a unit in F; proper and improper lattices always occur when 2 is not a unit. If 2 is a prime, $N(l)$ is $l \cdot l$ or $2(l \cdot l)$. For a π^i-modular l, we have $l \cdot l = \pi^i \mathfrak{o}$ and also

$$x \in Fl, x \notin l \Longrightarrow x \cdot l \supset \pi^i \mathfrak{o}.$$

It is easily seen that $l_1 \oplus l_2$ is π^i-modular if and only if l_1 and l_2 are π^i-modular. Also that $\pi^\lambda \circ l$ is $\pi^{i+\lambda}$-modular if l is π^i-modular. And l is unimodular if and only if $l \cdot l \subseteq \mathfrak{o}$ with $d(l)$ a unit. Any l with $l \cdot l \subseteq \mathfrak{o}$ is called totally integral.

Every l has a decomposition $l = l_1 \oplus \cdots \oplus l_t$ in which the l_λ are modular with $l_{\lambda+1} \cdot l_{\lambda+1} \subset l_\lambda \cdot l_\lambda$. We call this a Jordan decomposition of l. If $l = \oplus l_\lambda'$ is another such decomposition, then (i) it too must have t modular components, (ii) $l_\lambda \cdot l_\lambda = l_\lambda' \cdot l_\lambda'$, (iii) l_λ and l_λ' are both proper or both improper, (iv) $\dim l_\lambda = \dim l_\lambda'$. We go on to say any two lattices l, l' have the same type if their Jordan forms satisfy these four properties. We have proved in [9] that if l contains a π^i-modular lattice J, where $\pi^i \mathfrak{o} = l \cdot l$, then J is a component of L.

Definition. *Put* $\mathfrak{R} l = \{x \in Fl \mid x \cdot l \subseteq \mathfrak{o}\}$.

Proposition 5. *If l has Jordan form $l = \oplus l_\lambda$, then $\mathfrak{R} l = \oplus (\pi^{-s(\lambda)} l_\lambda)$, where $\pi^{s(\lambda)}\mathfrak{o} = l_\lambda \cdot l_\lambda$. In particular, $\mathfrak{R} l$ is a lattice.*

As consequences, we have $\mathfrak{R}\,\mathfrak{R}l = l$, and $\mathfrak{R}\,(l \oplus l') = \mathfrak{R}l \oplus \mathfrak{R}l'$.

PROPOSITION 6. *If* $\dim l = \dim L$, then $l \rightarrow L$ *if and only if* $\mathfrak{R}L \rightarrow \mathfrak{R}l$.

Since it is possible to give constructive methods for finding a Jordan form, we can always assume that a lattice is given in Jordan form when necessary.

Notation. $\bigoplus_{\varphi} l_\lambda = 0$, $\bigoplus_{\varphi} V_\lambda = 0$.

DEFINITION. *Let* $l = \oplus\, l_\lambda$ *be a Jordan form. Define* $\mathfrak{l}_i = \oplus\, l_\mu$ *where* μ *extends over values for which* $l_\mu \cdot l_\mu \supseteq \pi^i\mathfrak{o}$. *Let* $\mathfrak{l}_i{}^{\perp} = \oplus\, l_\mu$ *where* μ *extends over values for which* $l_\mu \cdot l_\mu \subset \pi^i\mathfrak{o}$.

Clearly $\mathfrak{l}_i = 0$ and $\mathfrak{l}_i{}^{\perp} = l$ if $l_1 \cdot l_1 \subset \pi^i\mathfrak{o}$, while $\mathfrak{l}_i = l$ and $\mathfrak{l}_i{}^{\perp} = 0$ if $l_t \cdot l_t \supseteq \pi^i\mathfrak{o}$. And $l = \mathfrak{l}_i \oplus \mathfrak{l}_i{}^{\perp}$ for any i. In the case of a lattice $L = \oplus\, L_\lambda$, we use $\mathfrak{L}_i$, $\mathfrak{L}_i{}^{\perp}$ instead. All these quantities depend not only on the lattice but also on the Jordan form.

In this chapter we have been establishing our basic ideas and interpreting the classical problem geometrically. Many of the ideas have already appeared in print and fuller details with proofs and references can be found in [9].

II. When 2 is a Unit.

Throughout this chapter, we shall assume that 2 is a unit in the basic field F. We start with an investigation that will lead to necessary conditions for a representation $l \rightarrow L$. Then we prove these conditions sufficient.

DEFINITION. *Let* $\mathfrak{p}$ *be any ideal in* F. *We say that* $l \rightarrow L \bmod \mathfrak{p}$ *if there is an* $\mathfrak{o}$*-linear map* ϕ *of* l *into* L *such that*

$$(\phi x)^2 \equiv x^2 \bmod \mathfrak{p} \qquad \textit{for all } x \in L.$$

It follows from the equation $x : y = \tfrac{1}{2}\{(x+y)^2 - x^2 - y^2\}$ *that* $\phi x \cdot \phi y \equiv x \cdot y \bmod \mathfrak{p}$.

PROPOSITION 7. *Let* $l = l_1 \oplus \cdots \oplus l_t$ *be a Jordan form. If* $l \rightarrow L \bmod \mathfrak{p}$ *with* $\mathfrak{p} \subset l_t \cdot l_t$, *then* $l \rightarrow L$.

Proof. Every lattice over a field of this type has an orthogonal basis, hence we can write $l = \mathfrak{o}z \oplus k$ with $z^2\mathfrak{o} = l \cdot l$. Let $x \rightarrow \bar{x}$ denote a representation of l into $L \bmod \mathfrak{p}$, so that $x^2 \equiv \bar{x}^2 \bmod \mathfrak{p}$. If $\dim k = 0$ we are through by Hensel's lemma, so assume $\dim k > 0$ and proceed by induction to $\dim l$.

We know that $\bar{l}$ is spanned by $\mathfrak{o}\bar{z}$ and $\bar{k}$; define

$$K = \{\bar{x} - ((\bar{x}\cdot\bar{z})/\bar{z}^2)\bar{z} \mid x \in k\}.$$

Since $x \cdot z = 0$, we have $\bar{x}\cdot\bar{z} \in \mathfrak{p}$, hence $(\bar{x}\cdot\bar{z})/\bar{z}^2 \in \pi\mathfrak{o}$. It follows that K is a lattice, that $\mathfrak{o}\bar{z}$ and K span $\bar{l}$, that $\mathfrak{o}\bar{z}\cdot K = 0$, and hence that $\bar{l} = \mathfrak{o}\bar{z} \oplus K$. Now define ϕ on k by

$$\phi x = \bar{x} - ((\bar{x}\cdot\bar{z})/\bar{z}^2)\bar{z}.$$

We see that ϕ is $\mathfrak{o}$-linear. And $(\phi x)^2 \equiv x^2 \bmod \mathfrak{p}$. Hence $k \rightarrow K \bmod \mathfrak{p}$. By the induction, $k \rightarrow K$. But $\mathfrak{o}z \rightarrow \mathfrak{o}\bar{z}$ by Hensel's lemma. Hence $l \rightarrow \bar{l} \subseteq L$. q. e. d.

PROPOSITION 8. *Let* $l = \oplus\, l_\lambda$, $L = \oplus\, L_\lambda$ *be Jordan forms. If* $l \rightarrow L$, *then* $\mathfrak{l}_i \rightarrow \mathfrak{L}_i$ *for all* i.

Proof. We have $l = \mathfrak{l}_i \oplus \mathfrak{l}_i{}^\perp$, $L = \mathfrak{L}_i \oplus \mathfrak{L}_i{}^\perp$. Let $\phi\colon (l \rightarrow L)$ be a representation. Define a mapping ψ on $\mathfrak{l}_i$ in the following way: for each $x \in \mathfrak{l}_i$, write $\phi x = \psi x + z$ with $\psi x \in \mathfrak{L}_i$, $z \in \mathfrak{L}_i{}^\perp$. It is easily verified that ψ is $\mathfrak{o}$-linear. Since $z^2 \in \pi^{i+1}\mathfrak{o}$ we have

$$x^2 = (\phi x)^2 \equiv (\psi x)^2 \bmod \pi^{i+1}.$$

Hence $\mathfrak{l}_i \rightarrow \mathfrak{L}_i \bmod \pi^{i+1}$. Hence $\mathfrak{l}_i \rightarrow \mathfrak{L}_i$ by Proposition 7. q. e. d.

LEMMA. *Let* l *be* π-*modular, and let* $L = L_1 \oplus L_2$ *have* L_1 *unimodular and* L_2 π-*modular or* 0. *If* $Fl \rightarrow FL$, *then* $l \oplus J_1 \oplus J_2 \rightarrow L$, *where* J_1 *is unimodular or* 0, J_2 *is* π-*modular or* 0, *and* $\dim(l \oplus J_1 \oplus J_2) = \dim L$.

Proof. We can suppose that $l \subseteq FL$. Since $\mathcal{R}l$ is π^{-1}-modular by Proposition 5, we can find a π^{-1}-maximal lattice $J \supseteq \mathcal{R}l$. But $\mathcal{R}l$ is then a component of J, hence $J = \mathcal{R}l \oplus \mathcal{R}J_2 \oplus \mathcal{R}J_1$ with $\mathcal{R}J_2$ π^{-1}-modular or 0, and $\mathcal{R}J_1$ unimodular or 0. Now let $K \supseteq \mathcal{R}L_1 \oplus \mathcal{R}L_2$ be π^{-1}-maximal. Then $K \cong J$ by Proposition 4. Hence

$$\mathcal{R}L_1 \oplus \mathcal{R}L_2 \rightarrow K \rightarrow \mathcal{R}l \oplus \mathcal{R}J_2 \oplus \mathcal{R}J_1,$$

so the result follows by Proposition 6. q. e. d.

THEOREM 1. *Let* $l = \oplus\, l_\lambda$ *and* $L = \oplus\, L_\lambda$ *be Jordan forms. Then* $l \rightarrow L$ *if and only if* $F\mathfrak{l}_i \rightarrow F\mathfrak{L}_i$ *for all* i.

Necessity. By Proposition 8 we have $\mathfrak{l}_i \rightarrow \mathfrak{L}_i$, hence $F\mathfrak{l}_i \rightarrow F\mathfrak{L}_i$ for all i.

Sufficiency. The proof is by induction to $\dim L$. Taking large enough i shows that $\dim l \leqq \dim L$. Taking an i with $l_1 \cdot l_1 = \pi^i\mathfrak{o}$ shows that $l_1 \cdot l_1$

$\subseteq L_1 \cdot L_1$. We suppose that $\dim l > 0$. First let $\dim L = 1$. Then $\dim l = 1$. Let l be π^i-modular. Then $Fl = F\mathfrak{l}_i \to F\mathfrak{L}_i$ so that $FL = F\mathfrak{L}_i$. Hence $l \to L$.

Now let $\dim L > 1$. First suppose that $l_1 \cdot l_1 \subseteq \pi^2(L_1 \cdot L_1)$. Define

$$L' = (\pi L_1) \oplus L_2 \oplus \cdots \oplus L_\lambda \oplus \cdots.$$

Put $\pi^j\mathfrak{o} = l_1 \cdot l_1$. Then for $i < j$, we have $F\mathfrak{l}_i = 0$ so that $F\mathfrak{l}_i \to F\mathfrak{L}_i'$; while for $i \geqq j$ we have $F\mathfrak{L}_i = F\mathfrak{L}_i'$ and again $F\mathfrak{l}_i \to F\mathfrak{l}_i'$. So l, L' satisfy the conditions of the theorem. Repeating this, we arrive at L'' with l, L'' still satisfying the conditions of the theorem, with $L'' \subseteq L$, and with $\pi^2(L'' \cdot L'') \subset l \cdot l$. In effect, this allows us to assume that $\pi(L_1 \cdot L_1) \subseteq l_1 \cdot l_1 \subseteq L_1 \cdot L_1$. By suitably scaling Fl and FL, we can assume that $L_1 \cdot L_1 = \mathfrak{o}$; then $l_1 \cdot l_1$ is $\mathfrak{o}$ or $\pi\mathfrak{o}$.

Case 1. $l_1 \cdot l_1 = \mathfrak{o}$. Then $l_1 = \mathfrak{l}_0$ and $L_1 = \mathfrak{L}_0$. So $Fl_1 \to FL_1$, and we have a replica of l_1 in FL_1. Let $J \supseteq l_1$ be $\mathfrak{o}$-maximal in FL_1. Then $J \cong L_1$ by Proposition 4 since L_1 is also $\mathfrak{o}$-maximal. So there is a replica $\bar{l}_1$ of l_1 in L_1. Now $\bar{l}_1$ is a component of L_1 since $\bar{l}_1$ is unimodular, hence $L_1 = \bar{l}_1 \oplus J_1$ with J_1 unimodular or 0. Define $L' = J_1 \oplus \mathfrak{L}_0{}^{\perp}$ and $l' = \mathfrak{l}_0{}^{\perp}$. For $i \leqq 0$, we have $F\mathfrak{l}_i' = 0 \to F\mathfrak{L}_i'$. For $i > 0$, we have

$$Fl_1 \oplus F\mathfrak{l}_i' = F\mathfrak{l}_i \to F\mathfrak{L}_i = F\bar{l}_1 \oplus F\mathfrak{L}_i',$$

and so $F\mathfrak{l}_i' \to F\mathfrak{L}_i'$ by Proposition 2. Hence $l' \to L'$ by the induction, hence $l \to L$.

Case 2. $l_1 \cdot l_1 = \pi\mathfrak{o}$. Then $l_1 = \mathfrak{l}_1$. By the lemma we have $\bar{l}_1 \oplus J_1 \oplus J_2 \subseteq \mathfrak{L}_1$ where $\bar{l}_1 \cong l_1$, J_1 is unimodular or 0, and J_2 is π-modular or 0. Define $L' = J_1 \oplus J_2 \oplus \mathfrak{L}_1{}^{\perp}$ and $l' = \mathfrak{l}_1{}^{\perp}$. For $i \leqq 1$ we have $F\mathfrak{l}_i' = 0 \to F\mathfrak{L}_i'$. For $i > 1$ we have

$$Fl_1 \oplus F\mathfrak{l}_i' = F\mathfrak{l}_i \to F\mathfrak{L}_i = F\bar{l}_1 \oplus F\mathfrak{L}_i'.$$

Hence $F\mathfrak{l}_i' \to F\mathfrak{L}_i'$ for all i. Hence $l' \to L'$ by the induction, hence $l \to L$. q. e. d.

III. When 2 is a Prime.

We now assume that 2 is a prime in the basic field F, so that the residue class field $\mathfrak{o}/(2\mathfrak{o})$ is a finite field of characteristic 2. Since $\operatorname{char} F \neq 2$, it follows [1] that F is a finite extension of the 2-adic numbers. Since the residue class field is finite it must have a quadratic extension, hence there are units ϵ, δ such that $x^2 + \epsilon x + \delta$ is irreducible modulo 2, hence there is a unit $\rho = \delta\epsilon^{-2}$ such that $x^2 + x + \rho$ is irreducible in F, hence

$$1 - 4\rho \notin (F^*)^2. \tag{2}$$

Now let ρ' be another unit for which $1-4\rho' \notin (F^*)^2$. Then $x^2+x+\rho'$ is irreducible, so $x^2+x+\rho'$ is irreducible modulo 2 by Hensel's lemma [1]. Let α be a root of $x^2+x+\rho$ in the quadratic extension of $\mathfrak{o}/(2\mathfrak{o})$; then we have $a \in \mathfrak{o}/(2\mathfrak{o})$ and a non-zero $b \in \mathfrak{o}/(2\mathfrak{o})$ such that $a+\alpha b$ solves $x^2+x+\rho'$; thus

$$a^2+\alpha^2 b^2+a+\alpha b+\rho'=0;$$

but $\alpha^2+\alpha+\rho=0$, so that $a^2+a+b^2\rho+\rho'=0$ and $b^2=b$; hence $b=1$ and so

$$x^2+x+(\rho+\rho')\equiv 0 \bmod 2$$

has a solution a in $\mathfrak{o}$. Hence

$$(1-4\rho)(1-4\rho')\equiv 1-4(\rho+\rho')\equiv(1+2a)^2 \bmod 8.$$

By Hensel's lemma, we therefore have

$$(1-4\rho)/(1-4\rho')\in(F^*)^2. \tag{3}$$

To sum up, if ρ and ρ' are integers (and therefore units) for which $1-4\rho$ and $1-4\rho'$ are non-squares, then $1-4\rho'$ is a square times $1-4\rho$. Accordingly, we fix the quantity ρ from now on and we use it to describe all non-squares of the form $1+4\alpha$ with $\alpha\in\mathfrak{o}$.

Modular classification. In this section we explicitly determine all unimodular lattices. The 1-dimensional ones are easily found, with $L\cong(\epsilon)$ being typical. We therefore examine higher dimensions.

TABLE I

	L	$d(L)$	L^2	$(FL)^2$
$H(0)$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$	-1	$2\mathfrak{o}$	F
$B(0)$	$\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}$	-1	$\mathfrak{u}\cup 4\mathfrak{o}$	F
$H(\rho)$	$\begin{pmatrix}2 & 1\\1 & 2\rho\end{pmatrix}$	$-1+4\rho$	$2\mathfrak{u}\mathfrak{o}^2$	$2\mathfrak{u}F^2$
$B(\rho)$	$\begin{pmatrix}1 & 1\\1 & 4\rho\end{pmatrix}$	$-1+4\rho$	$\mathfrak{u}\mathfrak{o}^2$	$\mathfrak{u}F^2$
$\Xi(\epsilon,\delta)$	$\begin{pmatrix}\epsilon & 1\\1 & 2\delta\end{pmatrix}$			

Binary case. We write down in a table a list of different binary lattices and give (without proof) the sets of numbers represented by them. We shall then prove that the table exhausts all binary unimodular lattices.
In the table, ϵ, δ are units. We shall not need L^2 and $(FL)^2$ in the last case. Note that two Ξ's may be isometric for different values of ϵ, δ.

PROPOSITION 9. *Every binary unimodular lattice is isometric to exactly one of the five lattices listed in Table I.*

Proof. By looking at the $d(L)$ and L^2 columns of Table I, we see that no two of the lattices can be isometric. Consider an arbitrary binary unimodular lattice K. Referring to the special basis given in (13) of [9], we see that

$$K \cong \begin{pmatrix} \epsilon & 1 \\ 1 & 2\alpha \end{pmatrix} \text{ or } K \cong \begin{pmatrix} 2\epsilon & 1 \\ 1 & 2\alpha \end{pmatrix}$$

with ϵ a unit and $\alpha \in \mathfrak{o}$. If $d(K) = -1$, then $FK \cong FB(0) \cong FH(0)$ so that $K \cong H(0)$ or $K \cong B(0)$ by Theorem 4.4 of [8]. If $N(K) = \mathfrak{o}$ with $d(K) = -1 + 4\rho$, it is easily verified that $1 \in K^2$ and so $K \cong B(\rho)$. If $N(K) = 2\mathfrak{o}$ with $d(K) = -1 + 4\rho$, it is easily verified that $2 \in K^2$ and so $K \cong H(\rho)$ by Theorem 14.3 of [8]. Finally, there is the possibility that $d(K) = -1 + 2\beta$ with β a unit; a determinantal consideration then shows that ϵ and α are units, hence $K \cong \Xi(\epsilon, \alpha)$. q. e. d.

Ternary case. Again referring to (13) of [9], we see that any ternary unimodular K has the form

$$K \cong H(0) \oplus (\epsilon) \text{ or } K \cong H(\rho) \oplus (\epsilon), \tag{4}$$

where ϵ is a unit. By Table I, the second of these is anisotropic; while the first is isotropic. Hence K can have exactly one of the decompositions appearing in (4). Once K is decomposed, the value of ϵu^2 is uniquely determined. Thus (4) gives a complete description of the ternary case.

Quaternary case. Here, as in the binary case, we start by giving a table of lattices and we then prove that every unimodular quaternary lattice appears exactly once. Again use ϵ, δ for units.

TABLE II

(i)	$H(0) \oplus B(0)$	$H(0) \oplus H(0)$	(ia)
(ii)	$H(0) \oplus B(\rho)$		
(iii)	$H(\rho) \oplus B(0)$	$H(\rho) \oplus H(0)$	(iiia)
(iv)	$H(\rho) \oplus B(\rho)$		
(v)	$H(0) \oplus \Xi(\epsilon, \delta)$		

PROPOSITION 10. *Every quaternary unimodular lattice is isometric to exactly one of the lattices in Table II. We have*

$$FH(0) \oplus FB(0) \cong FH(0) \oplus FH(0) \text{ and } FH(\rho) \oplus FB(0) \cong FH(\rho) \oplus FH(0).$$

With these exceptions, all lattices in the table generate non-isometric spaces.

Proof. The stated F-isometries are obvious. Let us first prove the last part. A determinantal argument rules out all space isometries of (i) except, possibly, with (iv); this is impossible since $FH(\rho) \ominus FB(\rho)$ is anisotropic by Table I. Similarly, (ii) reduces to proving that $FH(0) \oplus FB(\rho)$ and $FH(\rho) \oplus FB(0)$ cannot be isometric, and this follows from Witt's theorem and Table I. The remaining cases follow from determinantal arguments. So the last part is proved.

Now we prove there are no lattice isometries in the table. The previous discussion reduces this to proving that $H(0) \oplus B(0) \ncong H(0) \oplus H(0)$ and $H(\rho) \oplus B(0) \ncong H(\rho) \oplus H(0)$; both these relations follow by taking norms.

Finally, we prove that every quarternary unimodular L appears in the table. By (13) of [9], we can write $L = H(\alpha) \oplus J$ with $\alpha = 0$ or ρ and J binary; this establishes the result except when $\alpha = \rho$ and $J \cong \Xi(\epsilon, \delta)$ or $J \cong H(\rho)$, in which case we use (12) of [10] and the obvious isometry $H(\rho) \oplus H(\rho) \cong H(0) \oplus H(0)$. q. e. d.

Higher dimensions. Any such unimodular L has a decomposition $L = (\oplus H(0)) \oplus K$ in which K is ternary or quaternary, again by (13) of [9]. By Proposition 3 of [9], the lattice K is unique to an isometry.

Representation modulo $\mathfrak{p}$. Let $\mathfrak{p}$ be any $\mathfrak{o}$-ideal in F and let $\mathfrak{q}$ stand either for $\mathfrak{p}$ or for $\frac{1}{2}\mathfrak{p}$. We write

$$l \rightarrow L \bmod (\mathfrak{p}, \mathfrak{q}) \tag{5}$$

if there is an $\mathfrak{o}$-linear map ϕ of l into L such that

$$(\phi x)^2 \equiv x^2 \bmod \mathfrak{p}, \qquad \phi x \cdot \phi y \equiv x \cdot y \bmod \mathfrak{q}.$$

If $\mathfrak{q} = \mathfrak{p}$, we write $l \rightarrow L \bmod \mathfrak{p}$. If ϕ is an isomorphism onto, we write $l \cong L \bmod (\mathfrak{p}, \mathfrak{q})$ and $l \cong L \bmod \mathfrak{p}$ respectively. We note that if

$$\phi_1 : (l_1 \rightarrow L_1 \bmod \mathfrak{p}, \mathfrak{q}) \text{ and } \phi_2 : (l_2 \rightarrow L_2 \bmod \mathfrak{p}, \mathfrak{q}),$$

then there is a unique extension of ϕ_1, ϕ_2 to $\phi : (l_1 \oplus l_2 \rightarrow L_1 \oplus L_2 \bmod \mathfrak{p}, \mathfrak{q})$. If ϕ_1, ϕ_2 are one-one, then so is ϕ. If ϕ_1, ϕ_2 are onto, then so is ϕ.

PROPOSITION 11. *Let* l *and* L *be unimodular and suppose that* $N(l) = N(L)$ *and* $\dim l = \dim L$. *Then* $l \cong L \bmod 2$.

Proof. By Theorem 2.4 of [8], we can write l and L in canonical bases $\langle x \rangle$, $\langle y \rangle$ respectively. If $N(l) = \mathfrak{o}$ this means that both $\langle x \rangle$ and $\langle y \rangle$ are orthogonal bases, and we can assume that $x_\lambda{}^2 \equiv 1 \equiv y_\lambda{}^2 \bmod 2$. If $N(l) \subset \mathfrak{o}$, this means that $\mathfrak{o}x_{2\lambda-1} + \mathfrak{o}x_{2\lambda} \cong H(\alpha)$ so that we have $x_\lambda{}^2 \equiv 0 \equiv y_\lambda{}^2 \bmod 2$ and $x_\lambda \cdot x_\mu = y_\lambda \cdot y_\mu$. The $\mathfrak{o}$-linear map sending x_λ to y_λ is an isometry modulo 2. q. e. d.

LEMMA. *Let* $l = l_1 \oplus l_2$ *be totally integral with* l_1 *unimodular and either 1-dimensional or 2-dimensional improper. Suppose that* $\phi \colon (l \rightarrow L \bmod \mathfrak{p}, \mathfrak{q})$ *with* $\mathfrak{q} \subset \mathfrak{o}$. *Then* ϕl_1 *is unimodular and has the same type as* l_1, *and there is a decomposition* $\phi l = \phi l_1 \oplus l_2{}^*$ *with a representation* $l_2 \rightarrow L \bmod (\mathfrak{p}, \mathfrak{q})$ *of* l_2 *onto* $l_2{}^*$.

Proof. The proof that ϕl_1 has the same type as l_1 is left to the reader. Let us write $\phi x = \bar{x}$. First we suppose that $l_1 = \mathfrak{o}x$ so that $\bar{l}_1 = \mathfrak{o}\bar{x}$. Define

$$l_2{}^* = \{\bar{z} - ((\bar{x} \cdot \bar{z})/\bar{x}^2)\bar{x} \mid z \in l_2\}.$$

Then $l_2{}^* \subseteq \bar{l} \subseteq L$ is a lattice, $\bar{l}_1$ and $l_2{}^*$ span $\bar{l}$, and $\bar{l}_1 \cdot l_2{}^* = 0$ so that $\bar{l}$ is the direct sum of $\bar{l}_1$ and $l_2{}^*$; hence $\bar{l} = \bar{l}_1 \oplus l_2{}^*$. The mapping

$$\psi z = \bar{z} - ((\bar{x} \cdot \bar{z})/\bar{x}^2)\bar{x}$$

is the required representation of l_2 onto $l_2{}^* \bmod (\mathfrak{p}, \mathfrak{q})$.

Now let l_1 be improper, so that $l_1 = \mathfrak{o}x + \mathfrak{o}y$ and $\bar{l}_1 = \mathfrak{o}\bar{x} + \mathfrak{o}\bar{y}$. Define

$$l_2{}^* = \{\bar{z} + \alpha\bar{x} + \beta\bar{y} \mid z \in l_2\},$$

where $\alpha \in \mathfrak{q}$, $\beta \in \mathfrak{q}$ are given by

$$\alpha = \frac{\bar{y}^2(\bar{x} \cdot \bar{z}) - (\bar{x} \cdot \bar{y})(\bar{y} \cdot \bar{z})}{(\bar{x} \cdot \bar{y})^2 - \bar{x}^2\bar{y}^2}, \qquad \beta = \frac{\bar{x}^2(\bar{y} \cdot \bar{z}) - (\bar{x} \cdot \bar{y})(\bar{x} \cdot \bar{z})}{(\bar{x} \cdot \bar{y})^2 - \bar{x}^2\bar{y}^2}.$$

Then $l_2{}^* \subseteq \bar{l} \subseteq L$ is a lattice, $\bar{l}_1$ and $l_2{}^*$ span $\bar{l}$, and $\bar{l}_1 \cdot l_2{}^* = 0$ so that $\bar{l}$ is the direct sum of $\bar{l}_1$ and $l_2{}^*$; hence $\bar{l} = \bar{l}_1 \oplus l_2{}^*$. The mapping $\psi z = \bar{z} + \alpha\bar{x} + \beta\bar{y}$ is the required representation of l_2 onto $l_2{}^* \bmod (\mathfrak{p}, \mathfrak{q})$. This proves the lemma.

PROPOSITION 12. *Let* l *be unimodular and suppose that* $l \rightarrow L \bmod (\mathfrak{p}, \mathfrak{q})$ *under the mapping* ϕ *with* $\mathfrak{p} \subseteq 8/N(l)$. *Then* $l \cong \phi l$.

Proof. Using the fact that l has a canonical basis [8], we can find a decomposition $l = l_1 \oplus l_2$ of the type of the lemma such that $l_2 = 0$ or

$N(l_1) = N(l_2) = N(l)$. First let $l_2 = 0$. If l_1 is proper, the result follows from Hensel's lemma. If l_1 is improper, we observe that $l_1 \cong H(\alpha)$, $\bar{l}_1 \cong H(\beta)$, $d(l_1) = d(\bar{l}_1)$, so that $l_1 \cong \bar{l}_1$ by Table I. The general case follows by induction, using the lemma. q. e. d.

PROPOSITION 13. *Let* $l \rightarrow L \bmod (\mathfrak{p}, \mathfrak{q})$ *under the mapping* ϕ *with* l *unimodular and* $\mathfrak{q} \subset \mathfrak{o}$. *Then* $\dim \phi l = \dim l$, ϕl *is unimodular, and* $\phi l \cong l \bmod \mathfrak{p}$.

Proof. If we take $x \in l$, $x \notin 2l$, it is a consequence of the modularity of l that $\phi x \neq 0$, hence ϕ is one-one, so that $\dim l = \dim \bar{l}$. It is easily seen that $\bar{l}$ is unimodular and that $N(l) = L(\bar{l})$.. First let l be improper. If $\mathfrak{p} = 2\mathfrak{o}$, we have $\mathfrak{q} = 2\mathfrak{o} = \mathfrak{p}$, hence $l \cong \bar{l} \bmod \mathfrak{p}$ by Proposition 11. If $\mathfrak{p} \subseteq 4\mathfrak{o}$, we have $l \cong \bar{l}$ by Proposition 12. Hence assume that l is proper. Write $l = l_1 \oplus l_2$ with l_1 1-dimensional. Apply the lemma and the result follows by induction. q. e. d.

PROPOSITION 14. *Let* l *and* L *be unimodular with* $l \cong L \bmod \mathfrak{p}$, *where* $\mathfrak{p} \subset \mathfrak{o}$. *Given any* x_0 *with* $x_0{}^2\mathfrak{o} = \mathfrak{p}$, *there is a* y_0 *with* $y_0{}^2\mathfrak{o} = \mathfrak{p}$ *such that* $l \oplus \mathfrak{o}x_0 = K \oplus \mathfrak{o}y_0$ *with* $K \cong L \bmod 2\mathfrak{p}$.

Proof. First let l be improper so that L is improper too. Both l and L have the same dimension since they are isomorphic. By Proposition 12, we can assume that $\mathfrak{p} = 2\mathfrak{o}$. By (13) of [9], we can write $l = \oplus H(\alpha)$, where the α's are 0 or ρ. Similarly, we have $L = \oplus H(\beta)$. Now it is easily seen that both $H(0)$ and $H(\rho)$ can be chosen as components of $H(\alpha) \oplus \mathfrak{o}z_0$ whenever $z_0{}^2\mathfrak{o} = 2\mathfrak{o}$. Hence $(\oplus H(\alpha)) \oplus \mathfrak{o}x_0$ has $\oplus H(\beta)$ as a component. This proves the improper case, so we now assume that l and L are proper. Write $l = l_1 \oplus l_2$ with l_1 1-dimensional, and $l_2 = 0$ or $N(l_2) = N(l_1) = N(l) = \mathfrak{o}$. By the lemma, $L = \bar{l}_1 \oplus l_2{}^*$ with $l_1 \cong \bar{l}_1 \bmod \mathfrak{p}$ and $l_2 \rightarrow l_2{}^* \bmod \mathfrak{p}$. By Proposition 13, this means that $l_2 \cong l_2{}^* \bmod \mathfrak{p}$. Now using the perfectness of the residue class field, we easily see that $l_1 \oplus \mathfrak{o}x_0 = K_1 \oplus \mathfrak{o}z_0$ with $K_1 \cong \bar{l}_1 \bmod 2\mathfrak{p}$. Using an inductive argument, we see that $l_2 \oplus \mathfrak{o}z_0 = K_2 \oplus \mathfrak{o}y_0$ with $K_2 \cong l_2{}^* \bmod 2\mathfrak{p}$. Hence $l \oplus \mathfrak{o}x_0 = K \oplus \mathfrak{o}y_0$ with $K \cong L \bmod 2\mathfrak{p}$. q. e. d.

PROPOSITION 15. *Let* $l = \bigoplus_{1}^{t} l_\lambda$ *be a Jordan form and suppose that* $l \rightarrow L \bmod (\mathfrak{p}, \mathfrak{q})$ *under* ϕ, *where* $\mathfrak{p} \subseteq \mathfrak{q} \subset l_t \cdot l_t$. *Then* ϕl *is non-degenerate and has the same type as* l *with a Jordan form* $\phi l = \bigoplus_{1}^{t} l_\lambda{}^*$ *in which* $l_\lambda{}^* \cong {}_\lambda \bmod \mathfrak{p}$.

Proof. By suitably scaling l and L, we can take l_1 unimodular. By Proposition 13, we can take $t > 1$. We proceed by induction to $\dim l$. Write

$l_1 = K_1 \oplus J_1$ with K_1 1-dimensional or improper 2-dimensional, and $J_1 = 0$ or $N(J_1) = N(K_1) = N(l_1)$; this is possible since l_1 has a canonical basis. This induces a decomposition $l = K_1 \oplus K_2$ in which K_2 has the Jordan form $K_2 = J_1 \oplus (\bigoplus_{2}^{t} l_\lambda)$ with J_1 possibly 0. We can then write $\phi l = \phi K_1 \oplus K_2^*$, and we have a representation $K_2 \to L \bmod (\mathfrak{p}, \mathfrak{q})$ of K_2 onto K_2^* by the lemma. Now $K_1 \cong \phi K_1 \bmod \mathfrak{p}$ with K_1 and ϕK_1 of the same type, by Proposition 13. By the induction, we have

$$K_2^* = J_1^* \oplus (\bigoplus_{2}^{t} l_\lambda^*)$$

with K_2^* non-degenerate and of the same type as K_2, $J_1^* \cong J_1 \bmod \mathfrak{p}$, and $l_\lambda^* \cong l_\lambda \bmod \mathfrak{p}$ for $\lambda \geqq 2$. Hence

$$\phi l = (\phi K_1 \oplus J_1^*) \oplus (\bigoplus_{2}^{t} l_\lambda^*)$$

with $\phi K_1 \oplus J_1^* \cong K_1 \oplus J_1 \cong l_1 \bmod \mathfrak{p}$. q. e. d.

Notation. Let $l = \oplus l_\lambda$, $L = \oplus L_\lambda$ be given Jordan forms. We have already defined the lattices $\mathfrak{l}_i$, $\mathfrak{l}_i^\perp$, $\mathfrak{L}_i$, $\mathfrak{L}_i^\perp$ in terms of these decompositions. We now put $\mathfrak{L}_{(i)} = \oplus L_\mu$, where the summation extends over all values of μ for which $N(L_\mu) \supseteq 2^i\mathfrak{o}$; and $\mathfrak{L}_{(i)}^\perp = \oplus L_\mu$ with $N(L_\mu) \subset 2^i\mathfrak{o}$. Thus we have $L = \mathfrak{L}_{(i)} \oplus \mathfrak{L}_{(i)}^\perp$ for any i. We could also define $\mathfrak{l}_{(i)}$, $\mathfrak{l}_{(i)}^\perp$ in the same way, but we will not need them for l. We define $\mathfrak{l}_{[i]} = \oplus l_\mu$, where μ extends over all values for which $l_\mu \cdot l_\mu \supseteq 2^i\mathfrak{o}$ and, in addition, that value of μ, if any, for which $l_\mu \cdot l_\mu = 2^{i+1}\mathfrak{o}$ with l_μ improper. We define $\mathfrak{l}_{[i]}^\perp = \oplus l_\mu$ with μ extending over all values for which $l_\mu \cdot l_\mu \subset 2^{i+1}\mathfrak{o}$ and, in addition, that value of μ, if any, for which $l_\mu \cdot l_\mu = 2^{i+1}\mathfrak{o}$ with l_μ proper. Thus we have $l = \mathfrak{l}_{[i]} \oplus \mathfrak{l}_{[i]}^\perp$. We see that

$$\mathfrak{L}_{(i)} = \mathfrak{L}_{i-1} \text{ or } \mathfrak{L}_i, \qquad \mathfrak{l}_{[i]} = \mathfrak{l}_i \text{ or } \mathfrak{l}_{i+1}. \tag{6}$$

We now define Δ_i for L in the following way. If L has a proper 2^{i+1}-modular component, put $\Delta_i = 2^{i+1}\mathfrak{o}$; failing this, put $\Delta_i = 2^{i+2}\mathfrak{o}$ if L has a proper 2^{i+2}-modular component; otherwise, put $\Delta_i = 0$. We define δ_i as the quantity Δ_i when computed for l instead of L. Put $D_i = d(\mathfrak{L}_i)\mathfrak{o}$ and $d_i = d(\mathfrak{l}_i)\mathfrak{o}$; if $\mathfrak{L}_i = 0$ put $D_i = 0$, and the same when $\mathfrak{l}_i = 0$. Using the invariance of the type of a lattice, we see that δ_i, Δ_i, d_i, D_i are independent of the Jordan forms that define them. We have

$$\Delta_i = 2^{i+1}\mathfrak{o} \text{ or } 2^{i+2}\mathfrak{o} \text{ or } 0.$$

If $\alpha \in F$, denote by $(\alpha) \oplus L$ the lattice $\mathfrak{o}x \oplus L$ with $x^2 = \alpha$; similarly, with a quadratic space U. For any ideal $\mathfrak{p} \subset F$, write $\mathfrak{p} \rightarrow U$ if there is an $\alpha \in U^2$ for which $\alpha\mathfrak{o} = \mathfrak{p}$. If $\mathfrak{p} = 0$, we always have $\mathfrak{p} \rightarrow U$; if $\mathfrak{p} \neq 0$, saying that $\mathfrak{p} \rightarrow U$ is the same as saying that U represents some number of ordinal $\operatorname{ord} \mathfrak{p}$. We shall write $\mathfrak{p} \rightarrow \beta$ if $\mathfrak{p} \rightarrow Fx$ with $x^2 = \beta$. It is of practical importance to be able to decide whether $\mathfrak{p} \rightarrow U$ or not, and we shall give a solution to this field problem at the end of the paper. In the meantime, we need the following result.

PROPOSITION 16. *If* $\dim U \geqq 3$, *then* $\mathfrak{p} \rightarrow U$.

Proof. Write $U = \oplus Fx_\lambda$ with $x_\lambda{}^2\mathfrak{o} = \mathfrak{o}$ or $x_\lambda{}^2\mathfrak{o} = 2\mathfrak{o}$; we can suppose that $\dim U = 3$. Then it clearly suffices to assume that $x_\lambda{}^2$ are either all units or all primes; and we can then scale things to make them all units. The result follows by applying (4) and Table I to the lattice $\oplus\, \mathfrak{o}x_\lambda$. q. e. d.

PROPOSITION 17. *If* $l \rightarrow L$, *there exists a* J *of dimension* $\dim L - \dim l$ *such that* $l \oplus J \rightarrow L$.

Proof. By Proposition 3, we can take $l \subseteq L$. Let $\langle x \rangle$ denote an orthogonal basis for $(Fl)^\perp$ such that $x_\lambda \in L$. Put $J = \oplus\, \mathfrak{o}x_\lambda$. q. e. d.

Lower type. One of the simplest invariants in the theory of isometry of lattices is the type of a lattice. This invariant does not characterize a quadratic lattice, but it lays a foundation on which to build other invariants. Motivated by this, we introduce a corresponding notion of "lower type" into the representation theory.

Definition. We say that l *has a lower type than* L *if the following hold for all* i:

(7) $$\dim \mathfrak{l}_i \leqq \dim \mathfrak{L}_i,$$

(8) $$d_iD_i \rightarrow 1 \qquad \textit{if } \dim \mathfrak{l}_i = \dim \mathfrak{L}_i,$$

(9) $$\delta_i \subseteq \Delta_i + 2^{i+2}\mathfrak{o} \textit{ and } \Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathfrak{o} \textit{ if } \dim \mathfrak{l}_i = \dim \mathfrak{L}_i,$$

(10) $$\Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathfrak{o} \textit{ if } \dim \mathfrak{L}_i - 1 = \dim \mathfrak{l}_i > 0 \textit{ and } d_iD_i \rightarrow 2^{i+1},$$

(11) $$\delta_i \subseteq \Delta_i + 2^{i+2}\mathfrak{o} \textit{ if } \dim \mathfrak{L}_i - 1 = \dim \mathfrak{l}_i > 0 \textit{ and } d_iD_i \rightarrow 2^i.$$

It is clear that the above definition is independent of the Jordan forms chosen. The relation $\delta_i \subseteq \Delta_i + 2^{i+2}\mathfrak{o}$ says that L has a proper 2^{i+1}-modular component if l does; similarly, $\Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathfrak{o}$ says that l has a proper 2^i-modular component if L does. The conditions (7)-(11) are elementary in the sense that one can determine by inspecting given Jordan forms when they are satisfied.

PROPOSITION 18. *Let* $l \rightarrow L$. *Suppose that* $j \geqq i$ *and that* $\mathfrak{l}_i$ *has the Jordan form* $\oplus\, l_\mu \neq 0$. *Then there exists a lattice* $\oplus\, l_\mu{}^*$ *with the same type as* $\oplus\, l_\mu$ *such that* $\oplus\, l_\mu{}^* \subseteq \mathfrak{L}_j$ *and* $l_\mu{}^* \cong l_\mu \bmod N(\mathfrak{L}_j{}^\perp)$.

Proof. We have $\mathfrak{l}_i \rightarrow l \rightarrow L$. Let ϕ denote the representation $\mathfrak{l}_i \rightarrow L$. Given any $x \in \mathfrak{l}_i$, write $\phi x = \psi x + z$ with $\psi x \in \mathfrak{L}_j$ and $z \in \mathfrak{L}_j{}^\perp$. It is easily verified that ψ is $\mathfrak{o}$-linear and provides a representation

$$\mathfrak{l}_i \rightarrow \mathfrak{L}_j \bmod \mathfrak{p}, \mathfrak{q},$$

where $\mathfrak{p} = N(\mathfrak{L}_j{}^\perp)$, $\mathfrak{q} \subset 2^j\mathfrak{o} \subseteq 2^i\mathfrak{o}$, and $\mathfrak{q}$ is $\mathfrak{p}$ or $\frac{1}{2}\mathfrak{p}$. Our result then follows from Proposition 15. q. e. d.

PROPOSITION 19. *If* $l \rightarrow L$, *then* l *has a lower type than* L.

Proof. Choose Jordan forms for L and l. Fix an integer i and put $\mathfrak{l}_i = \oplus\, l_\mu$. By Proposition 18, there is a lattice $\mathfrak{l}_i{}^* \subseteq \mathfrak{L}_i$ which has the same type as $\mathfrak{l}_i$. Hence $\dim \mathfrak{l}_i = \dim \mathfrak{l}_i{}^* \leqq \dim \mathfrak{L}_i$, and (7) is proved. To prove (8), we can assume that $d_i \neq 0$, hence that $\mathfrak{l}_i \neq 0$. Since $\mathfrak{l}_i$ and $\mathfrak{l}_i{}^*$ have the same type, we have $d_i = d_i{}^*$. But $d(\mathfrak{l}_i{}^*)d(\mathfrak{L}_i) \in (F^*)^2$ since $F\mathfrak{l}_i{}^* = F\mathfrak{L}_i$. Hence $d_iD_i \rightarrow 1$ so that (8) is proved.

To prove the second part of (9), we suppose, if possible, that $\Delta_{i-1} = 2^i\mathfrak{o}$ but $\delta_{i-1} \subseteq 2^{i+1}\mathfrak{o}$. Thus $\mathfrak{L}_i$ has a proper 2^i-modular component while $\mathfrak{l}_i$ does not. By Proposition 18, we can choose $\mathfrak{l}_i{}^* \subseteq \mathfrak{L}_i$ of the same type as $\mathfrak{l}_i$. Since $\dim \mathfrak{l}_i{}^* = \dim \mathfrak{L}_i$, we have $\mathcal{R}\mathfrak{L}_i \subseteq \mathcal{R}\mathfrak{l}_i{}^*$. But $N(\mathcal{R}\mathfrak{L}_i) = 2^{-i}\mathfrak{o}$ while $N(\mathcal{R}\mathfrak{l}_i{}^*) \subseteq 2^{-i+1}\mathfrak{o}$, which is impossible. Our supposition must therefore be rejected. Hence $\Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathfrak{o}$.

Now (10). Suppose, if possible, that $\Delta_{i-1} = 2^i\mathfrak{o}$ but $\delta_{i-1} \subseteq 2^{i+1}\mathfrak{o}$. By Proposition 18, there is a lattice $\mathfrak{l}_i{}^* \subseteq \mathfrak{L}_i$ with the same type as $\mathfrak{l}_i$. Let J denote a 1-dimensional lattice for which $F(\mathfrak{l}_i{}^* \oplus J) = F\mathfrak{L}_i$ and $\mathfrak{l}_i{}^* \oplus J \subseteq \mathfrak{L}_i$. Since $d_i = d_i{}^* \neq 0$, we have $d_i{}^*D_i \rightarrow 2^{i+1}$, and we can actually assume that $J = \mathfrak{o}x$ with $x^2\mathfrak{o} = 2^{i+1+2r}\mathfrak{o}$ for some $r > 0$. Then $\mathcal{R}\mathfrak{L}_i \subseteq \mathcal{R}J \oplus \mathcal{R}\mathfrak{l}_i{}^*$. Now $N(\mathcal{R}\mathfrak{l}_i{}^*) \subseteq 2^{-i+1}\mathfrak{o}$ while $N(\mathcal{R}\mathfrak{L}_i) = 2^{-i}\mathfrak{o}$. This is impossible since $N(\mathcal{R}J) = 2^{-i-1-2r}\mathfrak{o}$.

Finally, (11) and the first half of (9). We can assume that $l \subseteq L$; by taking a suitably scaled orthogonal basis for $(Fl)^\perp$, we can assume that $\dim l = \dim L$. Hence $\mathcal{R}L \rightarrow \mathcal{R}l$. We put $\mathcal{R}L = L'$, $\mathcal{R}l = l'$, and define $(\Delta_i) = \Delta_i$ if $\Delta_i = 2^{i+1}\mathfrak{o}$, $(\Delta_i) = 0$ otherwise. Similarly, define (δ_i). We see that $\delta_i \subseteq \Delta_i + 2^{i+2}\mathfrak{o}$ and $(\delta_i) \subseteq (\Delta_i)$ are equivalent; also, $\Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathfrak{o}$ and $(\Delta_{i-1}) \subseteq (\delta_{i-1})$. We have

$$(\Delta_{-i-2}') = 2^{-2i-2}(\Delta_i), \qquad (\delta_{-i-2}') = 2^{-2i-2}(\delta_i),$$

and also,

$$\mathfrak{R}\,\mathfrak{L}_i^{\perp} = \mathfrak{L}_{-i-1}', \qquad \mathfrak{R}\,\mathfrak{l}_i^{\perp} = \mathfrak{l}_{-i-1}'.$$

First we do (11). This is trivial when $\dim \mathfrak{L}_i = \dim L$, so we assume that $\dim \mathfrak{L}_i < \dim L$. The given conditions imply that $\dim \mathfrak{l}_{-i-1}' - 1 = \dim \mathfrak{L}_{-i-1}' > 0$ and $D_{-i-1}' d_{-i-1}' \rightarrow 2^{(-i-1)+1}$; applying (10), we see that $(\delta_{-i-2}') \subseteq (\Delta_{-i-2}')$, hence $(\delta_i) \subseteq (\Delta_i)$. We prove the first half of (9) in the same way, using the second half of (9) instead of (10). q. e. d.

The necessity. In this section we prove a series of propositions that lead to necessary conditions for our main theorem on the representation $l \rightarrow L$.

PROPOSITION 20. *If* $l \rightarrow L$, *then* $\mathfrak{l}_{[i]} \rightarrow \mathfrak{L}_{(i+2)}$ *and* $F\mathfrak{l}_{[i]} \rightarrow F\mathfrak{L}_{(i+2)}$.

Proof. Write $\mathfrak{l}_{[i]} = \oplus\, l_\mu$. Using (6) and Proposition 18, we see that there is a lattice $\oplus\, l_\mu^* \subseteq \mathfrak{L}_{(i+2)}$ with the same type as $\mathfrak{l}_{[i]}$ and such that $l_\mu^* \cong l_\mu \bmod 2^{i+3}$. It follows from Proposition 12 that $l_\mu^* \cong l_\mu$. Hence $\mathfrak{l}_{[i]} \rightarrow \mathfrak{L}_{(i+2)}$, hence $F\mathfrak{l}_{[i]} \rightarrow F\mathfrak{L}_{(i+2)}$. q. e. d.

LEMMA. *If* $l \rightarrow L$ *and* $\delta_i = 2^{i+2}\mathfrak{o}$, *then* $\mathfrak{l}_{[i]} \oplus (2^{i+2}\epsilon) \rightarrow \mathfrak{L}_{(i+2)}$ *for some unit* ϵ.

Proof. Take $x_0 \in \mathfrak{l}_{[i]}^{\perp}$ such that $x_0^2\mathfrak{o} = 2^{i+2}\mathfrak{o}$. Then $K = \mathfrak{l}_{[i]} \oplus \mathfrak{o}x_0 \rightarrow l \rightarrow L$. Let this representation of K into L be denoted by ϕ. For any $x \in K$, put $\phi x = \bar{x} + w$ with $\bar{x} \in \mathfrak{L}_{(i+2)}$ and $w \in \mathfrak{L}_{(i+2)}^{\perp}$. The mapping $x \rightarrow \bar{x}$ of K into $\mathfrak{L}_{(i+2)}$ is $\mathfrak{o}$-linear, and

$$\bar{x}^2 \equiv x^2 \bmod 2^{i+3}, \qquad \bar{x} \cdot \bar{y} \equiv x \cdot y \bmod 2^{i+2}.$$

From this follows

$$\bar{x}_0^2\mathfrak{o} = 2^{i+2}\mathfrak{o}, \qquad \bar{x}_0 \cdot \bar{z} \in 2^{i+2}\mathfrak{o} \text{ if } z \in \mathfrak{l}_{[i]}.$$

We define

$$J = \{\bar{z} - ((\bar{x}_0 \cdot \bar{z})/\bar{x}_0^2)\bar{x}_0 \mid z \in \mathfrak{l}_{[i]}\}.$$

It is easily verified that J is a lattice, that J and $\mathfrak{o}\bar{x}_0$ span $\bar{K}$, and that $\bar{x}_0 \cdot J = 0$, so that $\bar{K}$ is the direct sum of J and $\mathfrak{o}\bar{x}_0$, hence $\bar{K} = J \oplus \mathfrak{o}\bar{x}_0$. The mapping $z \rightarrow \bar{z} - ((\bar{x}_0 \cdot \bar{z})/\bar{x}_0^2)\bar{x}_0$ provides a representation modulo 2^{i+2} of $\mathfrak{l}_{[i]}$ onto J.

Let us now write $\mathfrak{l}_{[i]} = \oplus\, l_\mu$. Then $J = \oplus\, l_\mu^*$ with $l_\mu^* \cong l_\mu \bmod 2^{i+2}$ by

Proposition 15. By Proposition 14, we can therefore write $\bar{K} = (\oplus\, l_\mu{}^{**}) \oplus \mathfrak{o}y_0$ with $l_\mu{}^{**} \cong l_\mu \bmod 2^{i+3}$ and $y_0{}^2\mathfrak{o} = 2^{i+2}\mathfrak{o}$. By Proposition 12, we have $l_\mu{}^{**} \cong l_\mu$. Hence $\mathfrak{l}_{[i]} \oplus \mathfrak{o}y_0 \rightarrow \mathfrak{L}_{(i+2)}$. q. e. d.

PROPOSITION 21. *If* $l \rightarrow L$, *then* $\delta_i \rightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]}$.

Proof. If $\delta_i = 0$, the result follows from Proposition 20. If $\delta_i = 2^{i+2}\mathfrak{o}$, if follows from the lemma. So assume $\delta_i = 2^{i+1}\mathfrak{o}$. Thus l has a proper 2^{i+1}-modular component l_λ. If we write $\mathfrak{l}_{i+1} = \oplus\, l_\mu$, using (6) and Proposition 18, we find a lattice $\oplus\, l_\mu{}^{*} \subseteq \mathfrak{L}_{(i+2)}$ of the same type as $\mathfrak{l}_{i+1}$ and such that $l_\mu{}^{*} \cong l_\mu \bmod 2^{i+3}$. For $\mu < \lambda$, this means that $l_\mu{}^{*} \cong l_\mu$, hence $\mathfrak{l}_{[i]} \oplus l_\lambda{}^{*} \rightarrow \mathfrak{L}_{(i+2)}$; hence $\delta_i = 2^{i+1}\mathfrak{o} \rightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]}$. q. e. d.

PROPOSITION 22. *If* $l \rightarrow L$, *then* $\Delta_i \rightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]}$.

Proof. By Proposition 20, we can assume that $2^m\mathfrak{o} = \Delta_i \neq 0$, hence $2^m\mathfrak{o}$ is $2^{i+1}\mathfrak{o}$ or $2^{i+2}\mathfrak{o}$. Therefore $\mathfrak{L}_{(i+2)}$ must have a 2^m-modular proper component. Since $\mathfrak{l}_{[i]} \rightarrow \mathfrak{L}_{(i+2)}$, by Proposition 17, we have a lattice J for which $\dim J + \dim \mathfrak{l}_{[i]} = \dim \mathfrak{L}_{(i+2)}$ such that $\mathfrak{l}_{[i]} \oplus J \rightarrow \mathfrak{L}_{(i+2)}$. Since $\mathcal{R}\mathfrak{L}_{(i+2)}$ has a proper 2^{-m}-modular component, we have

$$2^{-m}\epsilon \rightarrow \mathcal{R}\mathfrak{L}_{(i+2)} \rightarrow \mathcal{R}J \oplus \mathcal{R}\mathfrak{l}_{[i]}$$

for some unit ϵ. Since $N(\mathcal{R}\mathfrak{l}_{[i]}) \subseteq 2^{-i}\mathfrak{o} \subset 2^{-m}\mathfrak{o}$, we have $2^{-m}\mathfrak{o} \rightarrow F(\mathcal{R}J)$, thus $\Delta_i \rightarrow FJ \cong \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]}$. q. e. d.

PROPOSITION 23. *If* $l \rightarrow L$ *with* $\mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]} \cong FH(0)$, *then* $\Delta_i\delta_i \subseteq \delta_i{}^2$.

Proof. Suppose that $\delta_i = 2^{i+2}\mathfrak{o}$ and $\Delta_i = 2^{i+1}\mathfrak{o}$. Then by the lemma, there is a unit ϵ such that $\mathfrak{l}_{[i]} \oplus (2^{i+2}\epsilon) \rightarrow \mathfrak{L}_{(i+2)}$. By Proposition 17, we have

$$\mathfrak{l}_{[i]} \oplus (2^{i+2}\epsilon) \oplus (-2^{i+2+2r}\epsilon) \rightarrow \mathfrak{L}_{(i+2)}$$

for some $r > 0$. Since $\mathfrak{L}_{(i+2)}$ has a 2^{i+1}-modular component, there is a unit δ for which

$$2^{-i-1}\delta \rightarrow (-2^{-i-2-2r}\epsilon) \oplus (2^{-i-2}\epsilon) \oplus \mathcal{R}\mathfrak{l}_{[i]}.$$

It is easily verified that this is impossible. q. e. d.

PROPOSITION 24. *If* $l \rightarrow L$, *then* $2^i(1 + 4\omega) \rightarrow (2^i \oplus \mathfrak{L}_{(i+1)})/\mathfrak{l}_i$ *for* $\omega = \rho$ *or* 0.

Proof. If $\mathfrak{l}_i = 0$, the proof is trivial. Accordingly, let $\mathfrak{l}_i$ have the Jordan form $\oplus\, l_\mu \neq 0$. By Proposition 18, there is a lattice $\mathfrak{l}_i{}^{*} \subseteq \mathfrak{L}_{(i+1)}$ of the same type as $\mathfrak{l}_i$ and with Jordan form $\oplus\, l_\mu{}^{*}$ in which $l_\mu{}^{*} \cong l_a \bmod 2^{i+2}$. By Proposition 14, we can find another decomposition $\oplus l_\mu{}^{**}$ of the same type such that

$$\oplus l_\mu{}^{*} \oplus (2^{i+2}) = \oplus l_\mu{}^{**} \oplus (2^{i+2}\epsilon),$$

where ϵ is a unit, $l_\mu{}^{**} \cong l_\mu \bmod 2^{i+3}$, and hence $l_\mu{}^{**} \cong l_\mu$. We therefore have

$$\mathfrak{l}_i \oplus (2^{i+2}\epsilon) \to \mathfrak{l}_i{}^{*} \oplus (2^{i+2}) \to \mathfrak{L}_{(i+1)} \oplus (2^{i+2}).$$

A determinantal argument shows that $\epsilon = 1$ or $1 + 4\rho$. Hence

$$F(\mathfrak{l}_i \oplus (2^{i}\epsilon)) \to F((2^{i}) \oplus \mathfrak{L}_{(i+1)}),$$

hence $2^{i}(1 + 4\omega) \to (2^{i} \oplus \mathfrak{L}_{(i+1)})/\mathfrak{l}_i$. q. e. d.

PROPOSITION 25. *If* $l \to L$, *then* $2^{i}(1 + 4\omega) \to (2^{i} \oplus \mathfrak{L}_{(i+1)})/\mathfrak{l}_{[i]}$ *for* $\omega = \rho$ *or* 0.

Proof. Along the same lines as the last proposition. q. e. d.

Representation by modular lattices. In this section, we determine all lattices represented by a given unimodular lattice L.

PROPOSITION 26. *Let* l *be a* 2^{i}*-modular lattice with* $\dim l \leqq 2$. *Then there exists a lattice* J *such that* $l \subset J \subset Fl$ *with* J 2^{i-2}*-modular when* $\dim l = 1$ *and* 2^{i-1}*-modular when* $\dim l = 2$; J *can be chosen proper when* l *is improper.*

Proof. The case $\dim l = 1$ is trivial. If $\dim l = 2$, we write $l = \mathfrak{o}x + \mathfrak{o}y$ with $x^2 = 2^{i}\alpha$, $x \cdot y = 2^{i}$, $y^2 = 2^{i+1}\beta$, where α and β are integers; we can take β a unit and $\alpha \in 2\mathfrak{o}$ when l is improper; the existence of such a basis follows from Table I. Put $J = \mathfrak{o}x + \mathfrak{o}(\frac{1}{2}y)$. This satisfies the condition required of it. q. e. d.

PROPOSITION 27. *If* l *is totally integral, there is a lattice* $J_1 \oplus J_2$ *such that* $l \subseteq J_1 \oplus J_2 \subset Fl$ *with* J_1 *unimodular or* 0 *and* J_2 *either* 0 *or* 1*-dimensional* 2*-modular.*

Proof. By looking at a canonical basis of each modular component of a Jordan decomposition of l, we see that $l = \oplus l_\lambda$ with the l_λ modular and $\dim l_\lambda \leqq 2$. The result follows from successive application of Proposition 26. q. e. d.

THEOREM 2. *Let* L *be unimodular and let* l *be totally integral with* $Fl \to FL$ *and* $N(l) \subseteq N(L)$. *Then* $l \to L$ *if and only if*

$$\text{(I)} \qquad \Delta_{-1} \to L/\mathfrak{l}_{[-1]},$$

(II) $L/\mathfrak{l}_{[-1]} \cong FH(0)$ *implies* $\Delta_{-1}\delta_{-1} \subseteq \delta_{-1}^2$.

Proof. The necessity is a consequence of Propositions 22 and 23. We prove the sufficiency. We can suppose that $l \subset Fl \subseteq FL$. By suitably scaling an orthogonal basis for $(Fl)^\perp$, we can find a lattice $J \subseteq (Fl)^\perp$ with $J \cdot J \subseteq 4\mathfrak{o}$ and such that $F(l \oplus J) = FL$. The values of $\mathfrak{l}_{[-1]}$ and δ_{-1} are the same for $l \oplus J$ as for l. In effect, this allows us to assume that $Fl = FL$ from the start. We make this assumption.

First we assume that L is improper. It is then easily verified that L is a 2-maximal lattice in FL. Since $N(l) \subseteq N(L)$, we can find a 2-maximal lattice J such that $l \subseteq J \subset FL$. But $J \cong L$ by Proposition 4. Hence $l \to J \to L$. Accordingly, we assume from now on that $N(L) = \mathfrak{o}$. We exclude the trivial case of $\dim L = 1$.

Let us suppose that l is unimodular too. If l is improper, we have

$$\mathfrak{o} = \Delta_{-1} \to L/\mathfrak{l}_{[-1]} = L/l = 0,$$

which is impossible. Hence l and L have the same type, hence they are isometric by Theorem 4.4 of [8]. From now on we assume that $\mathfrak{l}_0 \neq l$.

Case 1. $N(l) = \mathfrak{o}$. Let $J_1 \oplus J_2 \supseteq l$ be a lattice as in Proposition 27. On determinantal grounds, we have $J_2 = 0$. Then $l \to J_1$; but J_1 is proper unimodular, so it is isometric to L by Theorem 4.4 of [8]. Hence $l \to L$.

Case 2. $\dim L$ odd. As in Case 1, we can find a unimodular lattice $J_1 \supseteq l$. But $N(J_1) = \mathfrak{o}$ since $\dim J_1$ is odd. Hence $l \to J_1 \to L$ by Theorem 4.4 of [8].

From now on, we can therefore assume that L is proper with $\dim L$ even, that $\mathfrak{l}_0 = \mathfrak{l}_{[-1]}$ is either 0 or improper unimodular, and that $\dim \mathfrak{l}_0^\perp \geqq 2$ is also even.

Case 3. $\dim \mathfrak{l}_0^\perp \geqq 4$. By Proposition 27, we can find $J \supseteq \mathfrak{l}_0^\perp$ with J a 2-modular lattice. By the decomposition (13) of [9], we can write $J = J_1 \oplus J_2$ with $J_1 \cong 2 \circ H(\alpha)$, where α is 0 or ρ. By Proposition 26, we can find a unimodular binary proper $J_1^* \supset J_1$. Hence, using Proposition 27 on J_2, we find a unimodular proper $J^* \supset J$. Then,

$$l \to \mathfrak{l}_0 \oplus J \to \mathfrak{l}_0 \oplus J^* \cong L.$$

Case 4. $\dim L = 2$. In this case, $\mathfrak{l}_0$ must be 0. First let L be anisotropic. By Proposition 27, we can find a unimodular binary lattice $J \supseteq l$. Then $l \to J$. A glance at Table I shows that L is either a $B(\rho)$ or one of the $\Xi(\epsilon, \delta)$, hence the same with J. Hence $l \to J \to L$ by Theorem 4.4 of [8].

Now let L be isotropic, hence we have $L \cong B(0)$. In view of the above reduction, we have $l \cdot l \subseteq 2\mathfrak{o}$. If we had $N(l) = 2\mathfrak{o}$, we would have $\Delta_{-1}\delta_{-1} \supset \delta_{-1}^2$ with $L/\mathfrak{l}_{[-1]} \cong FH(0)$, which is contrary to our hypothesis. Hence $N(l) \subseteq 4\mathfrak{o}$. Let J be a 4-maximal lattice such that $l \subseteq J \subset FL$. Then $2 \circ H(0) \rightarrow L$ is also 4-maximal and we have

$$l \rightarrow J \cong 2 \circ H(0) \rightarrow L.$$

This completes Case 4.

We are left with a proper unimodular L which has $\dim L \geqq 4$ even, and an l with an improper unimodular component $\mathfrak{l}_0$ with $\dim \mathfrak{l}_0{}^{\perp} = 2$.

Case 5. $\dim \mathfrak{l}_0{}^{\perp} = 2$. First let $\dim L > 4$. Using (13) of [9], we have $L \cong H(0) \oplus L'$ and $l \cong H(0) \oplus l'$. It is easily verified that l', L' satisfy the given conditions of the theorem. In effect, this allows us to assume that $\dim L = 4$. We then have $\mathfrak{l}_0 \cong H(0)$ or $H(\rho)$. First we consider an L which is neither an $H(0) \oplus B(0)$ nor an $H(\rho) \oplus B(0)$ in Table II. By Proposition 27, we can find a unimodular $J \supseteq l$. Then J itself has the form of one of the lattices appearing in Table II. Since $FJ = FL$, it follows from Proposition 10 and Theorem 4.4 of [8] that $J \cong L$, hence $l \rightarrow J \rightarrow L$.

If $L \cong H(0) \oplus B(0)$ and $\mathfrak{l}_0 \cong H(\rho)$, then $\mathfrak{o} = \Delta_{-1} \rightarrow L/\mathfrak{l}_{[-1]} \cong FH(\rho)$, which is impossible by Table I. Similarly, if $L \cong H(\rho) \oplus B(0)$, we cannot have $\mathfrak{l}_0 \cong H(0)$. Thus we consider $L \cong H(\alpha) \oplus B(0)$ and $\mathfrak{l}_0 \cong H(\alpha)$ with $\alpha = 0$ or ρ. Now it is easily verified that if we cancel these $H(\alpha)$ from L and l, then $B(0)$ and $\mathfrak{l}_0{}^{\perp}$ continue to satisfy the conditions of the theorem. But the theorem has already been established when $\dim L = 2$. Hence $\mathfrak{l}_0{}^{\perp} \rightarrow B(0)$, hence $l \rightarrow L$. q. e. d.

Method of proof. We can now give the necessity of our representation theorem over unramified 2-adic fields. This is no more than a restatement of Propositions 21-25. In virtue of Proposition 19, there will be no loss of generality in stating the theorem for a lattice l of lower type than L. The use of the symbols $\mathfrak{L}, \mathfrak{l}$ in the theorem presupposes that L, l are given in Jordan form. *Notation.* Write $\alpha(1 + 4\omega) \rightarrow U$ if either $\alpha \rightarrow U$ or $\alpha(1 + 4\rho) \rightarrow U$.

Theorem 3. *Let l have a lower type than L. Then $l \rightarrow L$ if and only if the following conditions hold for all i:*

(I) $$\Delta_i \rightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]},$$

(II) $$\delta_i \rightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]},$$

(III) $$\mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]} \cong FH(0) \text{ implies } \Delta_i\delta_i \subseteq \delta_i^2,$$

$$\text{(IV)} \qquad 2^i(1+4\omega) \to (2^i \oplus \mathfrak{L}_{(i+1)})/\mathfrak{l}_i,$$

$$\text{(V)} \qquad 2^i(1+4\omega) \to (2^i \oplus \mathfrak{L}_{(i+1)})/\mathfrak{l}_{[i]}.$$

We are left with the task of proving the sufficiency. This will be done by an inductive argument on a quantity Φ to be introduced presently. Consider the lattice L given in Jordan form $L_1 \oplus \cdots \oplus L_T$. We put

$$\operatorname{len} L = \operatorname{ord} L_T \cdot L_T - \operatorname{ord} L_1 \cdot L_1.$$

For example, a modular lattice has length 0. We define

$$\Phi(L) = \dim L_1 + (\dim L)^2 + (\dim L)(\operatorname{len} L).$$

It is easily seen that

$$\text{(12)} \qquad \min_L \Phi(L) = 2,$$

and this minimum it attained if and only if $\dim L = 1$. Now consider another lattice L' in Jordan form $\oplus L_\lambda'$ and suppose that

$$\text{(13)} \qquad \dim L' \leqq \dim L, \operatorname{len} L' \leqq \operatorname{len} L, \dim L_1' \lesseqgtr \dim L_1.$$

Then it is easily verified that

$$\text{(14)} \qquad \dim L_1' < \dim L_1 \Rightarrow \Phi(L') < \Phi(L),$$

$$\text{(15)} \qquad \dim L' < \dim L \Rightarrow \Phi(L') < \Phi(L),$$

$$\text{(16)} \qquad \operatorname{len} L' < \operatorname{len} L \Rightarrow \Phi(L') < \Phi(L).$$

Let us consider two lattices l, L which satisfy the conditions of the theorem. By either I or II, we have $F\mathfrak{l}_{[i]} \to F\mathfrak{L}_{(i+2)}$. If we choose i large enough, we have $\mathfrak{l}_{[i]} = l$, $\mathfrak{L}_{(i+2)} = L$, hence $Fl \to FL$. It follows from (7) that $l \cdot l \subseteq L \cdot L$. It follows from (9) that $N(l) \subseteq N(L)$. Hence

$$\text{(17)} \qquad Fl \to FL, \qquad l \cdot l \subseteq L \cdot L, \qquad N(l) \subseteq N(L).$$

An elementary computation shows that $2^j \circ l$ has a lower type than $2^j \circ L$ and that

$$\text{(18)} \qquad 2^j \circ l, \quad 2^j \circ L \text{ satisfy I-V.}$$

If L is modular, following (18), we can assume it is unimodular. Then $L = \mathfrak{L}_{(-1-2)}$ so that $l \to L$ by Theorem 2. Hence

$$\text{(19)} \qquad l \to L \text{ if } L \text{ is modular.}$$

Now let l, L be the two lattices given in the theorem. We have to prove $l \rightarrow L$. If $\Phi(L) = 2$ the result holds by (19). We proceed by induction. Thus we assume that $l' \rightarrow L'$ whenever l', L' satisfy the conditions of the theorem with $\Phi(L') < \Phi(L)$. We must deduce from this that $l \rightarrow L$. By (18) and (19), we can assume that

$$(20) \qquad \operatorname{len} L > 0, \qquad L \cdot L = L_1 \cdot L_1 = \mathfrak{o}.$$

In consequence, $l \cdot l = l_1 \cdot l_1 \subseteq \mathfrak{o}$. The assumption (20) is made from now on. Once we have proved our theorem, it will follow from the necessity that the given conditions continue to hold if we vary the Jordan forms of l and L. For the time being, we will have to content ourselves with the following two weaker forms of this result.

Remark 1. Let $\oplus L_\lambda'$ be another Jordan decomposition of L in which just two components L_1, L_2 have been changed, and suppose that $N(L_2) = 2\mathfrak{o}$ and that $\mathfrak{l}_{[-1]} \rightarrow L_1'$. Then $\oplus L_\lambda'$ and $\oplus l_\lambda$ satisfy the conditions of the theorem.

Proof. Since the definition of lower type is independent of the Jordan from, we need only verify I-V. Of all quantities appearing in these conditions, the only ones to be affected by the new decomposition are $\mathfrak{L}_0$ and $\mathfrak{L}_{(0)}$. By inspection, I-III hold when $i = -2$, while for other values, there is nothing to prove since nothing is changed. Since $\mathfrak{l}_{-1} = 0$, condition IV is trivial when $i = -1$. Condition V with $i = -1$ follows from the fact that $F\mathfrak{l}_{[-1]}$ is a component of $F\mathfrak{L}_0' = FL_1'$. q. e. d.

Remark 2. Let $\oplus L_\lambda'$ be another Jordan form for L in which just two components L_1, L_k have been changed, and suppose that $N(L_k) = 4\mathfrak{o}$ and that $\mathfrak{l}_{[-1]} = 0$. Then $\oplus L_\lambda'$ and $\oplus l_\lambda$ satisfy the conditions of the theorem.

Proof. As in the last remark, we need only verify I-V. Of all quantities appearing in these conditions, the only ones that can change are

$$\mathfrak{L}_0, \mathfrak{L}_1, \mathfrak{L}_{(0)}, \mathfrak{L}_{(1)}.$$

Condition I must be examined at $i = -2, -1$, where it follows by inspection since $\mathfrak{l}_{[-1]} = 0 = \mathfrak{l}_{[-2]}$. If $i = -2$, $\mathfrak{d}_{-2}$ is either 0 or $\mathfrak{o}$ and II follows from (17). Similarly, for $i = -1$ when $\mathfrak{d}_{-1}$ is 0 or $\mathfrak{o}$. We consider $i = -1$ with $\mathfrak{d}_{-1} = 2\mathfrak{o}$; this is established at once using Proposition 16 and Table I, unless $\mathfrak{L}_{(1)}'$ is (ϵ') or $B(\rho)$, with ϵ' a unit. Now it is impossible to have $\mathfrak{L}_{(1)}' \cong (\epsilon')$, for then $\mathfrak{L}_{(1)} \cong (\epsilon)$ which contradicts the assumption $2\mathfrak{o} = \mathfrak{d}_{-1} \rightarrow \mathfrak{L}_{(1)}/\mathfrak{l}_{[-1]} \cong \epsilon$. If $\mathfrak{L}_{(1)}' \cong B(\rho)$, using the fact that $N(L_k) \subseteq 4\mathfrak{o}$ and referring to Table I, we find that $\mathfrak{L}_{(1)} \cong B(\omega)$ with $\omega = 0$ or ρ. It is impossible to have $\omega = 0$

by III; it is impossible to have $\omega=\rho$ by II. This establishes II for the new decomposition.

To do III when $i=-2$, just observe that $\Delta_{-2}\delta_{-2}\subseteq\delta_{-2}{}^2$ always. Suppose we have $\mathfrak{L}_{(1)}{}'/\mathfrak{l}_{[-1]}\cong FH(0)$ with $\Delta_{-1}=\mathfrak{o}$ and $\delta_{-1}=2\mathfrak{o}$. Then $\mathfrak{L}_{(1)}{}'\cong B(0)$. As above, this implies that $\mathfrak{L}_{(1)}\cong B(\omega)$ with $\omega=0$ or ρ. As above, this is impossible. This proves III.

Condition IV holds for the new decomposition when $i=-1$ since $\mathfrak{l}_{-1}=0$, so take $i=0$. Since $L_1\oplus L_k=L_1{}'\oplus L_k{}'$ with $N(L_k)=N(L_k{}')=4\mathfrak{o}$, we see by Proposition 24 that $(1+4\omega')\oplus FL_1\rightarrow(1)\oplus FL_1{}'$, hence

$$(1+4\omega')\oplus F\mathfrak{L}_{(1)}\rightarrow(1)\oplus F\mathfrak{L}_{(1)}{}',$$

$$(1+4\omega)\oplus F\mathfrak{l}_0\rightarrow(1)\oplus F\mathfrak{L}_{(1)}.$$

Now add these representations, observe that

$$(1+4\omega)\oplus(1+4\omega')\cong 1\oplus(1+4\omega''),$$

apply Proposition 2, and we find that

$$(1+4\omega'')\oplus F\mathfrak{l}_0\rightarrow(1)\oplus F\mathfrak{L}_{(1)}{}',$$

so that IV remains true. It is seen in exactly the same way that V is true. q. e. d.

Remark 3. Let $\mathfrak{l}_0=0$. Suppose that $L_1=J\oplus L_1{}'$ with J binary, and $L_1{}'$ possibly 0. Let $K\subseteq J$ be a binary 2-modular lattice and put

$$L'=L_1{}'\oplus K\oplus(\bigoplus_{\lambda\geqq 2}L_\lambda).$$

Then $l\rightarrow L$ if L' is such that

$$N(K)=4\mathfrak{o}\qquad\text{when }\mathfrak{l}_{[0]}\neq 0,\tag{21}$$

$$\delta_0\subseteq\Delta_0{}'+4\mathfrak{o}\qquad\text{when }L_1\text{ is binary},\tag{22}$$

$$\delta_{-1}\rightarrow F\mathfrak{L}_{(1)}{}',\tag{23}$$

$$\mathfrak{L}_{(i+2)}{}'/\mathfrak{l}_{[i]}\cong FH(0)\text{ implies }\Delta_i{}'\delta_i\subseteq\delta_i{}^2\text{ for }i=-1,0.\tag{24}$$

Proof. We shall first verify that l, L' satisfy the conditions of the theorem, and then apply the inductive hypothesis to them. By inspection, we find

$$\Delta_i{}'=\Delta_i\qquad\text{for }i\neq-2,-1,0,\tag{25}$$

$$F\mathfrak{L}_i{}'=F\mathfrak{L}_i\qquad\text{for }i\neq 0,\tag{26}$$

$$F\mathfrak{L}_{(i)}{}'=F\mathfrak{L}_{(i)}\qquad\text{for }i\neq 0,1.\tag{27}$$

We also have

$$(28) \qquad \Delta_0' = \Delta_0 \qquad \text{when } N(K) = 4\mathfrak{o},$$

$$(29) \qquad F\mathfrak{L}_{(1)}' \supseteq F\mathfrak{L}_{(1)} \qquad \text{when } N(K) = 2\mathfrak{o},$$

$$(30) \qquad D_i' = \alpha_i^2 D_i \qquad \text{with } \alpha_i \in F.$$

Note that $D_i' \neq 0$ for $i \geqq 1$.

We start by proving that l has a lower type than L'. Then (7) follows from (26) since $\dim \mathfrak{l}_0 = 0$, and (8) follows from (30) since $d_0 = 0$. The first half of (9) is immediate for $i \neq -2, -1, 0$, by (25) and (26); for $i = -2, -1$, it is trivial since $\mathfrak{l}_0 = 0$; for $i = 0$, it is simply (22). The second half of (9) is deduced from (25) and (26) when $i \neq -1, 0, 1$; for $i = -1$, it is trivial; for $i = 0$, it holds since $\Delta_{-1}' \subseteq 2\mathfrak{o}$ when $\dim \mathfrak{L}_0' = \dim \mathfrak{l}_0 = 0$; if $i = 1$ and $\mathfrak{l}_{[0]} \neq 0$, it follows from (21) and (28); if $i = 1$ and $\mathfrak{l}_{[0]} = 0$, then $\dim \mathfrak{l}_1 = \dim \mathfrak{L}_1' > 0$ so that l_1 is 2-modular proper, hence $\delta_0 = 2\mathfrak{o}$, hence $\Delta_0 \subseteq \delta_0 + 4\mathfrak{o}$. Using (25) and (26), we get (10) for $i \geqq 2$; if $i = 1$ and $\mathfrak{l}_{[0]} \neq 0$, this condition follows from (21); if $i = 1$ and $\mathfrak{l}_{[0]} = 0$, the condition $\dim \mathfrak{l}_1 > 0$ implies that l_1 is 2-modular and proper, hence $\Delta_0' \subseteq \delta_0 + 4\mathfrak{o}$. In proving (11), we can assume $i \geqq 1$ since $\dim \mathfrak{l}_i > 0$; the condition then follows by (26), (30) and (25). This proves that l has lower type than L'.

Now we verify I-III. For $i \neq -2, -1, 0$, they follow from (25) and (27). Condition I follows trivially for $i = -2, -1$ since $\mathfrak{l}_{[-2]} = \mathfrak{l}_{[-1]} = 0$; similarly for $i = 0$ if $\mathfrak{l}_{[0]} = 0$; if $\mathfrak{l}_{[-0]} \neq 0$, then

$$\Delta_0' = \Delta_0 \rightarrow \mathfrak{L}_{(2)}/\mathfrak{l}_{[0]} = \mathfrak{L}_{(2)}'/\mathfrak{l}_{[0]}.$$

Condition II follows from I when $i = -2$, since $\delta_{-2} = 0$; for $i = -1$, II is simply (23); for $i = 0$, it follows from (27). Since $\delta_{-2} = 0$, III holds when $i = -2$; for $i = -1, 0$ it is (24).

By (27), we must check IV for $i = -1, 0$. It is then trivial since $\mathfrak{l}_i = 0$. By (26), we must check V for $i = -1$; it is then trivial since $\mathfrak{l}_{[-1]} = 0$.

All this proves that l and L' satisfy the conditions of the theorem. Clearly $\dim L' = \dim L$, $\operatorname{len} L' \leqq \operatorname{len} L$; we also have $\dim L_1' < \dim L_1$ when $\dim L_1 > 2$, and $\operatorname{len} L' < \operatorname{len} L$ when $\dim L_1 = 2$. By (13), (14) and (16) this means $\Phi(L') < \Phi(L)$. By the induction, we have $l \rightarrow L$. Hence $l \rightarrow L' \rightarrow L$. q. e. d.

We now continue with the proof. Exactly one of three different things can happen to l. Either $\mathfrak{l}_{[0]} = 0$, or l_1 is unimodular, or l_1 is 2-modular improper. We find it convenient to consider these three possibilities separately in the rest of the proof.

When $\mathfrak{I}_{[0]} = 0$. In this section we find ourselves referring to Remark 3 a number of times. In doing so, it will be unnecessary to verify (21) since $\mathfrak{I}_{[0]} = 0$. The condition $\mathfrak{I}_0 = 0$ is also always true.

Case 1. L_1 proper, $\dim L_1 \geqq 3$. Then L_1 has an orthogonal basis; so by (4), we can write $L_1 = J \oplus L_1'$ with $J = \mathfrak{o}x + \mathfrak{o}y$, where $x^2 = 2$, $x \cdot y = 1$, $y^2 \in 2\mathfrak{o}$. In this case, $L_1' \neq 0$. Define $K = \mathfrak{o}x + \mathfrak{o}(2y)$. Define L' and apply Remark 3. Then (21), (22) are immediate. Since $\dim \mathfrak{L}_{(1)}' \geqq 3$, we have (23) in virtue of Proposition 16. Since $\dim \mathfrak{L}_{(i+2)}' \geqq 3$ and $\mathfrak{I}_{[i]} = 0$ for $i = -1, 0$, we have (24). Hence $l \rightarrow L$.

Case 2. $L_1 \cong \Xi(\epsilon, \delta)$. Write $L_1 = \mathfrak{o}x + \mathfrak{o}y = J$ with $y^2\mathfrak{o} = 2\mathfrak{o}$. Put $K = \mathfrak{o}(2x) + \mathfrak{o}y$. Define L' and apply Remark 3. We have $\Delta_0' = 2\mathfrak{o}$ so that (22) holds. Since $\delta_{-1} = 0$ or $2\mathfrak{o}$, and since L' has a proper 2-modular component, we have (23). A determinantal argument shows that $\mathfrak{L}_{(i+2)}'/\mathfrak{I}_{[i]}$ is not an $FH(0)$ for $i = -1, 0$, so that (24) holds. Hence $l \rightarrow L$.

Case 3. $L_1 \cong B(\alpha)$ with $\alpha = 0$ or ρ. First assume that $\Delta_0 = 2\mathfrak{o}$. Then we can write $L_1 \oplus L_2 = L_1' \oplus L_2'$ in such a way that $L_1 \cong \Xi(\epsilon, \delta)$ for some units ϵ, δ. By Remark 1, we see that $\oplus\, l_\lambda$ and $\oplus\, L_\lambda'$ satisfy the conditions of the theorem; hence $l \rightarrow L$ by Case 2. Accordingly, we now assume that $\Delta_0 \subseteq 4\mathfrak{o}$. Suppose that $\delta_0 = 2\mathfrak{o}$, so that $\delta_{-1} = 2\mathfrak{o}$ too. If $L_1 \cong B(\rho)$, we have $2\mathfrak{o} = \delta_{-1} \rightarrow \mathfrak{L}_{(1)}/\mathfrak{I}_{[-1]} \cong FB(\rho)$ which is impossible by Table I. If $L_1 \cong B(0)$, we have $\mathfrak{L}_{(1)}/\mathfrak{I}_{[-1]} \cong FH(0)$, hence $\Delta_{-1}\delta_{-1} \subseteq \delta_{-1}{}^2$, hence $\mathfrak{o} \cdot 2\mathfrak{o} \subseteq 4\mathfrak{o}$, which is false. Hence we deduce that $\delta_{-1} = 0$ and $\delta_0 \subseteq 4\mathfrak{o}$. We write $L_1 = J = \mathfrak{o}x + \mathfrak{o}y$ with $x^2 = 1$, $x \cdot y = 1$, $y^2 \in 4\mathfrak{o}$ and define $K = \mathfrak{o}(2x) + \mathfrak{o}y$. Define L' and apply Remark 3. Then (22) is immediate since $\delta_0 \subseteq 4\mathfrak{o}$. So is (23). So is (24) when $i = -1$; for $i = 0$, we have $\Delta_0' \subseteq 4\mathfrak{o}$, and therefore (24) holds. Hence $l \rightarrow L$.

Case 4. $L_1 \cong H(0)$, $\delta_0 = 4\mathfrak{o}$, $\Delta_0 \subseteq 4\mathfrak{o}$. We write $L_1 = \mathfrak{o}x + \mathfrak{o}y = J$ with $x^2 = 0 = y^2$, $x \cdot y = 1$. Put $K = \mathfrak{o}(2x) + \mathfrak{o}y$. Define L' and apply Remark 3. Then (21) and (22) are immediate. Since $\delta_{-1} = 0$, we have (23); for the same reason, we have (24) when $i = -1$; for $i = 0$, this condition follows from the fact that $\Delta_0' \subseteq 4\mathfrak{o}$. Hence $l \rightarrow L$.

Case 5. L_1 improper. By Case 4, we can assume that δ_0 is 0 or $2\mathfrak{o}$, or that Δ_0 is $2\mathfrak{o}$, when $L_1 \cong H(0)$. Write $L_1 = J \oplus L_1'$, $J = \mathfrak{o}x + \mathfrak{o}y$ with $x^2 = 2, x \cdot y = 1, y^2 \in 2\mathfrak{o}$. Put $K = \mathfrak{o}x + \mathfrak{o}(2y)$. Define L' and apply Remark 3. We see that $\Delta_0' = 2\mathfrak{o}$. Thus (21) and (22) are immediate. Since δ_{-1} is 0 or $2\mathfrak{o}$, we have (23). If $i = -1$, we have $\delta_{-1} = 0$ or $2\mathfrak{o}$ and $\Delta_{-1}' = 2\mathfrak{o}$, so that $\Delta_{-1}'\delta_{-1} \subseteq \delta_{-1}^2$; if $i = 0$ with $\mathfrak{L}_{(2)}'/\mathfrak{l}_{[0]} \cong FH(0)$, then $F\mathfrak{L}_{(2)}' \cong FH(0)$ so that $L_1 \cong H(0)$ and $\Delta_0 \subseteq 4\mathfrak{o}$; according to our assumptions on δ_0, Δ_0, we therefore have $\delta_0 = 0$ or $2\mathfrak{o}$. Hence (24) holds and $l \rightarrow L$.

Case 6. $\dim L_1 = 1$, $\operatorname{len} L = 1$. In this case, we have $L_1 \cong (\epsilon)$, and L_2 2-modular. By (17), we can take $l \subseteq FL$. First we assume that L_2 is proper. Since $\mathfrak{l}_{[0]} = 0$, any improper component l_μ of l must have $l_\mu \cdot l_\mu \subseteq 4\mathfrak{o}$. Using the fact that each l_μ has a canonical basis, we can write $l = \oplus J_\lambda$ with $\dim J_\lambda \leqq 2$, $J_\lambda \cdot J_\lambda \subseteq 2\mathfrak{o}$, and $J_\lambda \cdot J_\lambda \subseteq 4\mathfrak{o}$ when J_λ is improper. Suitably scaling an orthogonal basis for $(Fl)^\perp$ allows us to assume that we have a lattice $J = \oplus J_\lambda$ with the above properties and such that $l \subseteq J$, $FL = FJ$. Using Proposition 26, we can find $J' = J_1' \oplus J_2'$ with J_1', J_2' both proper, J_1' 2-modular or 0, J_2' 4-modular, and $J' \supseteq J$. On determinantal grounds, J_2' cannot be 0; indeed, $\dim J_2'$ must be odd. If $\dim L = 2$, $\dim J_2' = 1$; using (4) and Proposition 26 allows us always to take $\dim J_2' = 1$. Now put $L_2' = 2L_1$, $L_1' = L_2$. Then it is easily seen (one may apply Theorem 9.1 of [8]) that $L' \cong J'$. Hence

$$l \rightarrow J \rightarrow J' \rightarrow L' \rightarrow L.$$

We must now consider the case of an improper L_2. We put $L' = (2L_1) \oplus L_2$. It is easily seen that L' is 4-maximal. If we had $N(l) = 2\mathfrak{o}$, we would have $2\mathfrak{o} \rightarrow \delta_{-1} \rightarrow \mathfrak{L}_{(1)}/\mathfrak{l}_{[-1]} \rightarrow FL_1$, which is impossible. Hence $N(l) \subseteq 4\mathfrak{o}$, so we can find a 4-maximal lattice J with $l \subseteq J \subset FL$. But $L' \cong J$ by Proposition 4. Hence $l \rightarrow J \rightarrow L' \rightarrow L$. This proves Case 6.

Case 7. $\dim L_1 = 1$, $\operatorname{len} L > 1$. Thus $L_1 \cong (\epsilon)$ with ϵ a unit. We put $L' = (2L_1) \oplus L_2 \oplus \cdots$. But for a simple regrouping of terms, this gives a Jordan form for L'. It is easily seen that

$$\Delta_i' = \Delta_i \qquad \text{for } i \neq -2, -1, 0, 1, \tag{31}$$

$$F\mathfrak{L}_i' = F\mathfrak{L}_i \qquad \text{for } i \neq 0, 1, \tag{32}$$

$$F\mathfrak{L}_{(i)}' = F\mathfrak{L}_{(i)} \qquad \text{for } i \neq 0, 1, 2. \tag{33}$$

We also have

$$\Delta_1' = 4\mathfrak{o}, \Delta_0' \supseteq 4\mathfrak{o}, \tag{34}$$

$$F\mathfrak{L}_{(2)}' \supseteq F\mathfrak{L}_{(2)}, \tag{35}$$

$$D_i' = \alpha_i^2 D_i, \text{ with } \alpha_i \neq 0 \text{ if } i \geqq 2. \tag{36}$$

We are now going to prove that l and L' satisfy the conditions of the theorem. Our first task is to prove that l has a lower type than L'. Condition (7) must be verified for $i = 0, 1$; for $i = 0$, it is trivial since $\dim \mathfrak{l}_0 = 0$; if $\dim \mathfrak{L}_1 = \dim \mathfrak{l}_1 > 0$ we cannot have $d_1D_1 \rightarrow 1$, hence $\dim \mathfrak{L}_1 > \dim \mathfrak{l}_1$, hence $\dim \mathfrak{l}_1 \leqq \dim \mathfrak{L}_1'$. Condition (8) is immediate when $i \geqq 2$; if $\dim \mathfrak{L}_1' = \dim \mathfrak{l}_1$, the 2-modular components of l and L' have the same dimension, hence $d_1D_1 \rightarrow 1$. The first half of (9) follows from (31) and (32) when $i \geqq 2$; if $i = 1$, it follows from (34); if $\delta_0 = 2\mathfrak{o}$, we have $\delta_{-1} = 2\mathfrak{o}$ and so $\Delta_0' = \Delta_0 = 2\mathfrak{o}$ by II; if $i < 0$, $\delta_i \subseteq \Delta_i' + 2^{i+2}\mathfrak{o}$ since $\delta_i \subseteq 2\mathfrak{o}$. Similarly, the second part of (9) is immediate when $i \geqq 3$; consider $i = 2$ with $\dim \mathfrak{l}_2 = \dim \mathfrak{L}_2'$; then $\Delta_1' \subseteq \delta_1 + 8\mathfrak{o}$ if $\Delta_1' = \Delta_1$; so assume that $\Delta_1 \subseteq 8\mathfrak{o}$ and $\delta_1 \subseteq 8\mathfrak{o}$; this means that $\dim \mathfrak{L}_2 = \dim \mathfrak{l}_2$ with the 4-modular components of $\mathfrak{L}_2$ and $\mathfrak{l}_2$ either 0 or improper, and hence the dimensions of these components have the same parity; this means that the dimensions of the 2-modular components of $\mathfrak{L}_2$ and $\mathfrak{l}_2$ have opposite parity, and this denies (8); if $i = 1$ with $\Delta_0' = 2\mathfrak{o}$ and $\dim \mathfrak{l}_1 = \dim \mathfrak{L}_1'$, we see that $\dim \mathfrak{L}_1 - 1 = \dim \mathfrak{l}_1 > 0$ and $d_1D_1 = d_1D_1' \rightarrow 4$; hence $\Delta_0' = \Delta_0 \subseteq \delta_0 + 4\mathfrak{o}$ by (10); if $i = 0$ with $\dim \mathfrak{L}_0' = \dim \mathfrak{l}_0 = 0$, $\Delta_{-1}' \subseteq 2\mathfrak{o} \subseteq \delta_{-1} + 2\mathfrak{o}$; for $i < 0$, the condition is trivial. Hence (9) is completely verified. Condition (10) is immediate for $i \geqq 3$; consider $i = 2$ and suppose that $\dim \mathfrak{L}_2' - 1 = \dim \mathfrak{l}_2 > 0$ with $d_2D_2' \rightarrow 2^3$; if $\Delta_1 = 4\mathfrak{o}$ or $\delta_1 = 4\mathfrak{o}$, we are through; so assume that $\Delta_1 \subseteq 8\mathfrak{o}$ and $\delta_1 \subseteq 8\mathfrak{o}$; the dimensions of the 4-modular components of $\mathfrak{L}_2$ and $\mathfrak{l}_2$ must therefore have the same parity, hence the same is true for the 2-modular components, hence $d_2D_2 \rightarrow 1$, which contradicts $d_2D_2' \rightarrow 2^3$; for $i = 1$, we have $\delta_0 = 2\mathfrak{o}$ if $\dim \mathfrak{l}_1 > 0$ since $\mathfrak{l}_{[0]} = 0$; for $i < 1$, the condition (10) is trivial. For $i \geqq 2$, (11) follows from (31), (32), (36); for $i = 1$, it follows from (34); for $i < 1$, it is vacuous since $\dim \mathfrak{l}_i$ is then 0. We have therefore proved that l has a lower type than L'.

We are now going to prove

(37) $$\Delta_1' \rightarrow \mathfrak{L}_{(3)}/\mathfrak{l}_{[1]},$$

(38) $$\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]} \cong FH(0) \text{ implies } \Delta_1'\delta_1 \subseteq \delta_1^2.$$

If $\Delta_1 = 4\mathfrak{o}$, the results follow from (33), (34), I and III; if $\delta_1 = 4\mathfrak{o}$, they follow from (33), (34), and II. We therefore assume that $\Delta_1 \subseteq 8\mathfrak{o}$ and $\delta_1 \subseteq 8\mathfrak{o}$; thus the dimensions of the 4-modular components of $\mathfrak{L}_2$ and $\mathfrak{l}_2$ have the same parity and $\mathfrak{l}_2 = \mathfrak{l}_{[1]}$. By (8) l, L', we have $\dim \mathfrak{l}_2 < \dim \mathfrak{L}_2' = \dim \mathfrak{L}_2$. First let $\Delta_1 = 8\mathfrak{o}$. We can then assume that $\dim \mathfrak{l}_{[1]} = \dim \mathfrak{l}_2 = \dim \mathfrak{L}_2' - 1 = \dim \mathfrak{L}_2 - 1$, and that the 8-modular component of L is 1-dimensional, in virtue of Proposition 16. Then the dimensions of the 2-modular components of l, L have the same parity so that ord$(d(\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]}))$ is odd; here $F\mathfrak{l}_{[1]}\to F\mathfrak{L}_{(3)}$ by I; hence $\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]}$ is of the form $F(\epsilon\oplus 2\delta)$, hence (37) and (38) follow. We now assume that $\Delta_1=0$; in this case, $\mathfrak{L}_{(3)}=\mathfrak{L}_2$. By Proposition 16, we need only verify (37) and (38) for $\dim\mathfrak{L}_2-\dim\mathfrak{l}_2=1$ or 2. We still have $\mathfrak{l}_2=\mathfrak{l}_{[1]}$. If $\dim\mathfrak{L}_2-\dim\mathfrak{l}_2=1$, then (38) is vacuous; we prove (37); as before we see that the dimensions of the 2-modular components of $\mathfrak{L}_2$ and $\mathfrak{l}_2$ have the same parity, hence ord$(d(\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]}))$ is even; here $F\mathfrak{l}_{[1]}\to F\mathfrak{L}_{(3)}$ by I; hence $\Delta_1'\to\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]}$. We now assume that $\dim\mathfrak{L}_2=\dim\mathfrak{l}_2+2$. Using the above methods, we find that $\mathfrak{L}_{(3)}/\mathfrak{l}_{[1]}$ is of the form $F(\epsilon\oplus 2\delta)$ so that (37) and (38) follow.

Now we establish I-III for l, L'. For $i\geqq 2$, they are immediate. If $i=1$, we get I from (37) and (33); if $i\leqq 0$, the proof of I is trivial since $\mathfrak{l}_{[i]}$ is then 0. If $i=1$, II is trivial; if $i=0$, it follows from (35); if $i=-1$, we can take $\delta_{-1}=2\mathfrak{o}$, then $\delta_{-1}\to F\mathfrak{L}_{(1)}$ so that L has a 2-modular component, hence $\delta_{-1}\to F\mathfrak{L}_{(1)}'$; for $i\leqq -2$, II is trivial since δ_i is then 0. For $i=1$, III follows from (38); if $i=0$ and $\Delta_0'=2\mathfrak{o}$, then $F\mathfrak{L}_{(2)}'$ is not an $FH(0)$; if $i\leqq -1$, the condition is trivial since $\Delta_i'\subseteq 2\mathfrak{o}$. This proves I-III. By (33), it suffices to prove IV for $i=-1,0,1$; for $i=-1,0$ it is true since $\mathfrak{l}_i$ is then 0; for $i=1$, it follows from (35). Similarly with V.

We have therefore proved that l, L' satisfy the conditions of the theorem. Now $\dim L'=\dim L$ and $\operatorname{len} L'<\operatorname{len} L$ since $\operatorname{len} L>1$; hence by (16), we have $\Phi(L')<\Phi(L)$. Hence by the inductive assumption, we have $l\to L'\to L$.

When l_1 is unimodular. We shall divide the work into a number of cases as we did in the last section. All these cases have a certain computation in common which we now perform.

Remark 4. If $l_1\to L_1$, then $l\to L$.

Proof. We write $L_1=J\oplus L_1'$ with $J\cong l_1$ and $\dim L_1'\geqq 0$. If l_1 is proper and if L_1' is a $B(0)$, it is easily seen that we can find a new decomposition for L_1 of the above type and such that L_1 is an $H(0)$. So we can assume that

(39) L_1' is not a $B(0)$ if $N(l_1)=\mathfrak{o}$.

If L_1' is a $B(\rho)$ with $N(l_1)=\mathfrak{o}$ and $N(L_2)=4\mathfrak{o}$, referring to Remark 2 allows us to take a new decomposition for $L_1'\oplus L_2$ in which L_1' is a $B(0)$; utilizing (39), we can therefore assume that

(40) L_1' is not a $B(\alpha)$ if $N(l_1)=\mathfrak{o}$, $N(L_2)=4\mathfrak{o}$.

We define

$$L' = L_1' \oplus \Big(\bigoplus_{\lambda \geqq 2} L_\lambda\Big), \qquad l' = \bigoplus_{\lambda \geqq 2} l_\lambda .$$

It suffices to prove that $l' \to L'$.

First we establish that l' has a lower type than L'. It is evident that

$$(41) \qquad \Delta_i' = \Delta_i, \qquad \delta_i' = \delta_i \qquad \text{for } i \geqq 0,$$

$$(42) \qquad \dim \mathfrak{L}_i' - \dim \mathfrak{l}_i' = \dim \mathfrak{L}_i - \dim \mathfrak{l}_i \qquad \text{for all } i,$$

and that $d_i' = d_i$, $D_i' = D_i$ when $\mathfrak{l}_i' \neq 0$. Hence (7) and (8) hold for l', L'. The first half of (9) clearly holds for $i \geqq 0$; if $i \leqq -1$, it is true since δ_i' is then 0 or $2\mathfrak{o}$. The second half of (9) follows from (41), (42) when $i \geqq 1$; if $i = 0$, the condition on the dimensions implies that $\Delta_{-1}' \subseteq 2\mathfrak{o}$; if $i \leqq -1$, it is trivial. Both (10) and (11) are consequences of (41), (42) since the dimensional conditions imply that $i \geqq 1$. Hence l' has a lower type than L'.

Now we prove that l', L' satisfy I-V. It is easily seen that we have $F\mathfrak{l}_{[i]}' \to F\mathfrak{L}_{(i+2)}'$ and hence $\mathfrak{L}_{(i+2)}'/\mathfrak{l}_{[i]}' \cong \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]}$ for any $i \geqq 0$. Using (41), we therefore see that I-III hold for $i \geqq 0$. Similarly, IV and V hold for $i \geqq 0$. For $i \leqq -1$, we have $\mathfrak{l}_{[i]}' = 0$ and I is then easily deduced. Since $\delta_i' = 0$ for $i \leqq -2$, it suffices to consider II for $i = -1$ with $\delta_{-1}' = 2\mathfrak{o}$; this means that l has a proper 2-modular component and so $\delta_0 = 2\mathfrak{o} = \delta_0'$; if $\dim l_1 = \dim L_1$, we have $\delta_0 \subseteq \Delta_0 + 4\mathfrak{o}$ by (9), hence L' has a proper 2-modular component, hence $\delta_{-1}' \to F\mathfrak{L}_{(1)}'$; if $\dim l_1 + 1 = \dim L_1$, the result follows in the same way using (11); let $\dim l_1 + 2 = \dim L_1$; then II is immediate if $\Delta_0 = 2\mathfrak{o}$; if $N(L_2) = 4\mathfrak{o}$ and $N(l_1) = \mathfrak{o}$, it follows from (40); if $N(L_2) = 4\mathfrak{o}$ with $N(l_1) = 2\mathfrak{o}$, then

$$\delta_{-1}' = \delta_{-1} \to \mathfrak{L}_{(1)}/\mathfrak{l}_{[-1]} = L_1/l_1 \cong FL_1' \cong \mathfrak{L}_{(1)}'/\mathfrak{l}_{[-1]}';$$

it is impossible to have $L_1' \cong B(\rho)$ when $N(L_2) \subseteq 8\mathfrak{o}$ and $\delta_{-1}' = 2\mathfrak{o}$, for we then have

$$2\mathfrak{o} = \delta_0 \to \mathfrak{L}_{(2)}/\mathfrak{l}_{[0]} \cong FL_1' \cong FB(\rho);$$

when $\dim L_1 - \dim l_1 \geqq 3$, the condition is immediate by Proposition 16. Hence we have proved II.

For $i \leqq -2$, the proof of III is trivial since we then have $\delta_i' = 0$, so we consider $i = -1$; we can then assume that $\Delta_{-1}' = \mathfrak{o}$, $\delta_{-1}' = 2\mathfrak{o}$; then L' cannot have a 2-modular proper component, else we would not have $F\mathfrak{L}_{(1)}' \cong \mathfrak{L}_{(1)}'/\mathfrak{l}_{[-1]}' \cong FH(0)$; hence $\mathfrak{L}_{(1)}' \cong L_1' \cong B(0)$; by (39) l_1 must be improper and so $\delta_{-1} = 2\mathfrak{o}$; but this implies that $\mathfrak{L}_{(1)}/\mathfrak{l}_{[-1]} \cong \mathfrak{L}_{(1)}'/\mathfrak{l}_{[-1]}' \cong FH(0)$

which contradicts the original III. The proof of IV is immediate for $i \leqq -1$ since l_i' is then 0. The same with V.

We have therefore proved that l' and L' satisfy the conditions of the theorem. Now $\dim L' < \dim L$ and $\operatorname{len} L' \leqq \operatorname{len} L$, so that $\Phi(L') < \Phi(L)$ by (15). By the induction, we then have $l' \rightarrow L'$, hence $l \rightarrow L$. q. e. d.

We now consider the various cases. By (7), we always have $\dim l_1 \leqq \dim L_1$. In the first three cases, we shall assume that l_1 is proper, so by (17) we have L_1 proper too.

Case 1. $N(L_2) = 2o$. Write $L_1 = J \oplus L_1'$ with $\dim J = \dim l_1$, $N(J) = N(l_1)$ and L_1' proper or 0; since L_1 has a canonical basis, we can do this. By Proposition 11, we have $J \cong l_1 \bmod 2$. In virtue of Proposition 14 and Remark 1, we are entitled to assume that $J \cong l_1 \bmod 4$. If $\dim L_1' > 0$, L_1' must represent a unit ϵ, hence 4ϵ, hence by Propositions 14 and 12, we have $J' \cong l_1$. Hence $l \rightarrow L$ by Remark 4. We now assume that $L_1' = 0$. If $N(L_3) = 4o$, using Propositions 14 and 12 with Remark 2 allows us to take $J \cong l_1$, and so $l \rightarrow L$ by Remark 4. We proceed in the same way if L_2 represents 4ϵ with ϵ a unit, only this time we use Remark 1 again.

To complete this case, we must consider $l_1 \cong L_1 \bmod 4$ with L_2 representing no number 4ϵ, and $N(L_3) \subseteq 8o$. By (4), this means that $\dim L_2 \leqq 2$. By I, we have $F(l_1 \oplus 2\epsilon) \rightarrow F(L_1 \oplus L_2)$; using a determinantal argument when $\dim L_2 = 2$, we see that $F(l_1 \oplus L_2') \cong F(L_1 \oplus L_2)$ for some proper 2-modular L_2' with $\dim L_2' \leqq 2$. Hence $l_1 \oplus L_2' \cong L_1 \oplus L_2$ by Theorem 9.1 of [8]. Using Remark 1, we can assume that $l_1 \cong L_1$. Hence $l \rightarrow L$ by Remark 4.

Case 2. $N(L_2) = 4o$. It follows from IV that

$$F((1+4\omega) \oplus l_1) \rightarrow F(1 \oplus L_1).$$

Now write $L_1 = L_1' \oplus o x_0$ with $x_0^2 = \epsilon$ a unit. Since L_2 represents 4δ with δ a unit, it is easily seen that $o x_0 \oplus L_2 = o \bar{x}_0 \oplus \bar{L}_2$ with $\bar{x}_0^2 = \epsilon(1+4\omega)$; put $\bar{L}_1 = L_1' \oplus o\bar{x}_0$; then the Jordan form $\bar{L}_1 \oplus \bar{L}_2 \oplus L_3 \oplus \cdots$ continues to satisfy the conditions of the theorem by Remark 2. But $1 \oplus L_1 \cong (1+4\omega) \oplus \bar{L}_1$ and so $Fl_1 \rightarrow F\bar{L}_1$, hence $l_1 \rightarrow \bar{L}_1$ by Theorem 2, hence $l \rightarrow L$ by Remark 4.

Case 3. $N(L_2) \subseteq 8o$. Using I, we see that $Fl_1 \rightarrow FL_1$, hence $l_1 \rightarrow L_1$ by Theorem 2, hence $l \rightarrow L$ by Remark 4.

We have covered all cases with l_1 proper unimodular. Now consider l_1 improper; then L_1 may or may not be improper; but it follows from (9) that L_1 is improper whenever $\dim l_1 = \dim L_1$.

Case 4. $N(L_2)=2\mathfrak{o}$. Using the fact that $\dim l_1<\dim L_1$ when $N(L_1)=\mathfrak{o}$, and referring to the decomposition of a unimodular lattice that is given in (12)-(14) of [9], it is easily seen that we can write $L_1=J\oplus L_1'$ with $\dim J=\dim l_1$ and $N(J)=N(l_1)$; L_1' may be 0. Then $J\cong l_1 \bmod 2$ by Proposition 11. By Propositions 14 and 12, we can write $J\oplus L_2=J'\oplus L_2'$ with $l_1\cong J'$; by Remark 1, we can assume that actually $l_1\cong J$. Hence $l\to L$ by Remark 4.

Case 5. $N(L_2)\subseteq 4\mathfrak{o}$. Since $\Delta_{-1}\to\mathfrak{L}_{(1)}/\mathfrak{l}_{[-1]}$, we have $\Delta_{-1}\to L_1/l_1$, hence $Fl_1\to FL_1$. We know $N(l_1)\subseteq N(L_1)$. Apply Theorem 2 to l_1, L_1. Then

$$\Delta_{-1}(L_1)=\Delta_{-1} \text{ or } 0, \qquad \delta_{-1}(l_1)=0;$$

hence the first condition of Theorem 2 is satisfied; the second one is trivial. Hence $l_1\to L_1$. Hence $l\to L$ by Remark 4.

When l_1 is 2-modular improper. We continue on the same lines as in the last two sections. First we perform some computations, then we apply them to the different cases that follow.

Remark 5. Let m be a binary component of l_1 and let M be a binary component of L_1 or L_2. If $m\to M$, then $l\to L$.

Proof. Clearly m is either a $2\circ H(0)$ or a $2\circ H(\rho)$. If M is 2-modular, then $m\cong M$. If M is unimodular, then M is a $B(0)$, $B(\rho)$ or $H(0)$. Let $L_a=M\oplus L_a'$; a is then 1 or 2. Put $L_\lambda'=L_\lambda$ for $\lambda\neq a$ and define L' by the Jordan form $L'=\oplus L_\lambda'$. Define l' in the same way by putting $l_1=m\oplus l_1'$. We see that

$$\delta_i'=\delta_i \text{ for all } i, \qquad \Delta_i'=\Delta_i \text{ for } i\geqq 0, \tag{43}$$

$$\delta_0=0 \text{ or } 4\mathfrak{o}, \qquad \delta_i=0 \text{ for } i\leqq -1. \tag{44}$$

We also have $\dim\mathfrak{L}_i'-\dim\mathfrak{l}_i'=\dim\mathfrak{L}_i-\dim\mathfrak{l}_i$ when $i\geqq 1$. Also $d_i=4d_i'$, $D_i=\alpha D_i'$, with $\alpha=1$ or 4, when $\mathfrak{l}_i'\neq 0$. Using this information, it is clear that l' has a lower type than L'. Now,

$$\mathfrak{L}_{(i+2)}'/\mathfrak{l}_{[i]}'\cong\mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]} \qquad \text{if } i\geqq 0. \tag{45}$$

Using (43), (44), (45), it is evident that I-III hold for l', L'. Similarly, IV and V. We omit the details as quite straight-forward; there are none of the technical difficulties that we encountered with this kind of proof earlier on. Hence l', L' satisfy the conditions of the theorem. But $\dim L'<\dim L$,

$\operatorname{len} L' \leqq \operatorname{len} L$; hence $\Phi(L') < \Phi(L)$ by (15), hence $l' \to L'$ by the induction, hence $l \to L$. q. e. d.

Remark 6. *If* $FB(\alpha) \to FL_1$, then $l \to L$.

Proof. If L_1 is proper, using Theorem 2, we see that $B(\alpha) \to L_1$ so that $J \cong B(\alpha)$ is a component of L_1. If L_1 is improper, α must be 0 when $\dim L_1 = 2$ so that $J \cong H(0)$ is a component of L_1; for higher dimensions, the last remark is always true. In both cases, we can therefore write $L_1 = J \oplus L_1'$ with $J \cong B(\alpha)$ or $H(0)$. Define $K \subset J$ such that $K \cong 2 \circ H(\beta)$. Apply Remark 3. Then (21)-(24) are easily verified, hence $l \to L$. q. e. d.

Case 1. $N(L_2) = 2\mathrm{o}$. First let $\dim L_1 \geqq 2$. Using Table I, equation (4), and Propositions 11 and 14, we see that $L_1 \oplus L_2$ has another Jordan form $L_1' \oplus L_2'$ with L_1' representing one of $H(0)$, $B(0)$, $B(\rho)$. By Remark 1, we know that $\oplus L_\lambda'$, $\oplus l_\lambda$ satisfy the conditions of the theorem. Hence $l \to L$ by Remark 6. Now let $\dim L_1 = 1$ so that L_1 is proper. If $\dim L_2 \geqq 3$, it is easily seen that we can write $L_1 \oplus L_2$ in the Jordan form $L_1' \oplus L_2'$ with L_2' representing either $2 \circ H(0)$ or, if we wish, $2 \circ H(\rho)$. By Remark 1, $\oplus L_\lambda'$ and $\oplus l_\lambda$ satisfy the conditions of the theorem. By Remark 5, we have $l \to L$. We cannot have $\dim L_1 = 1$ with $\dim L_2 \leqq 2$ in virtue of (8) and (10).

Case 2. L_2 improper 2-modular. First let L_1 be proper. It is easily seen that we can write $L_1 \oplus L_2 = L_1' \oplus L_2'$ with $2 \circ H(0) \to L_2'$ or, if we wish, $2 \circ H(\rho) \to L_2'$. By Remark 2, $\oplus L_\lambda'$ and $\oplus l_\lambda$ continue to satisfy the conditions of the theorem. By Remark 5, we therefore have $l \to L$. We now take L_1 improper. By Remark 6, we can take $L_1 \cong H(\rho)$; by Remark 5, we can take $L_2 \cong 2 \circ H(\alpha)$, $l_1 \cong 2 \circ H(\beta)$ with $\alpha = 0$ or ρ, $\beta = 0$ or ρ, and $\alpha \neq \beta$. If $N(L_3) = 4\mathrm{o}$, it follows from Propositions 11, 12 and 14 that $L_2 \oplus L_3 = L_2' \oplus L_3'$ with $L_2' \cong 2 \circ H(\beta)$; it is easily verified that the new Jordan forms satisfy the conditions of the theorem. (None of the earlier technical difficulties arise in dong this.) Hence $l \to L$ by Remark 5. We therefore assume that $N(L_3) \subseteq 8\mathrm{o}$. By I, we have $F\mathfrak{l}_{[0]} \to F\mathfrak{L}_{(2)}$, hence $F(2 \circ H(\beta)) \to FH(\rho) \oplus F(2 \circ H(\alpha))$, hence $FB(\beta) \to FH(\rho) \oplus FB(\alpha)$. If $\alpha = \rho$, we have $\beta = 0$, hence $FB(0)$ is isotropic but $FH(\rho) \oplus FB(\rho)$ is not; so this is impossible. If $\alpha = 0$, we have $\beta = \rho$ and $FB(\rho) \oplus FH(0) \cong FH(\rho) \oplus FB(0)$, and this is impossible by Table II and Proposition 10.

Case 3. $L_2 \cdot L_2 \subseteq 4\mathrm{o}$. First let L_1 be proper. If $N(L_2) \subseteq 8\mathrm{o}$, then $Fl_1 \to FL_1$ by I. If $N(L_2) = 4\mathrm{o}$, we have $F((1 + 4\omega) \oplus l_1) \to F(1 \oplus L_1)$

by V. Put $L_1 = L_1' \oplus \mathfrak{o}x_0$ with $x_0^2 = \epsilon$ where ϵ is a unit. Then $\mathfrak{o}x_0 \oplus L_2 = \mathfrak{o}\bar{x}_0 \oplus \bar{L}_2$ with $\bar{x}_0^2 = \epsilon(1 + 4\omega)$. Put $\bar{L}_1 = L_1' \oplus \mathfrak{o}\bar{x}_0$. Then $\bar{L}_1 \oplus \bar{L}_2 \oplus L_3 \oplus \cdots$ and $\oplus\, l_\lambda$ still satisfy the conditions of the theorem by Remark 2. Since $(1) \oplus L_1 \cong (1 + 4\omega) \oplus \bar{L}_1$, this implies that $Fl_1 \to F\bar{L}_1$. So we take it that $Fl_1 \to FL_1$ when L_1 is proper. Hence $FB(\alpha) \cong F(2 \circ H(\alpha)) \to FL_1$, hence $l \to L$ by Remark 6. Now let L_1 be improper. By Remark 6, we can assume that $L_1 \cong H(\rho)$. So $l_1 \cong 2 \circ H(\alpha)$ with $\alpha = 0$ or ρ. By V, we then have $F((1 + 4\omega) \oplus B(\alpha)) \to F(1 \oplus H(\rho))$; this is impossible since the first of these spaces is isotropic while the second is not.

We have now completed the proof of Theorem 3.

IV. Practical Aspects.

The central feature in all our tests (Theorems 1-3) is the notion of space representation. It is therefore important to be able to determine when $U \to V$. Solutions are available in the literature ([6], [12]), so we merely give a summary here. Consider the quadratic spaces U, V over the local field F. Put $\operatorname{def} = \dim V - \dim U$ and assume that $\operatorname{def} \geqq 0$. Let SU, SV denote Hasse symbols of U, V. Then for spaces of the same dimension,

$$U \cong V \Leftrightarrow dU = dV, SU = SV.$$

And $U \to V$ if and only if

$\operatorname{def} = 0$: $U \cong V$,

$\operatorname{def} = 1$: $U \oplus (dU \cdot dV) \cong V$,

$\operatorname{def} = 2$: $dU \cdot dV = -1$ implies $U \oplus FH(0) \cong V$,

$\operatorname{def} \geqq 3$: none.

This gives us all we need to carry out the test in Theorem 1. We therefore assume that $2 \in F$ is a prime. We have to answer the following questions: when is $V/U \cong W$? When is $\alpha \to V/U$? When is $\mathfrak{p} \to V/U$? The answers to the first two questions are $U \oplus W \cong V$, and $(\alpha) \oplus U \to V$, respectively. We consider when $\mathfrak{p} \to V/U$. We can assume that $\mathfrak{p} \neq 0$, $\operatorname{def} > 0$, and $U \to V$. If $\dim V/U = 1$, we have $\mathfrak{p} \to V/U$ if and only if $\operatorname{ord} \mathfrak{p}$ and $\operatorname{ord}(dV \cdot dU)$ have the same parity. If $\dim V/U \geqq 2$, we have $\mathfrak{p} \to V/U$ if and only if

$$U \oplus FB(\rho) \cong V \text{ implies } \operatorname{ord} \mathfrak{p} \text{ even},$$

$$U \oplus FH(\rho) \cong V \text{ implies } \operatorname{ord} \mathfrak{p} \text{ odd}.$$

THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] E. Artin, *Algebraic Numbers and Algebraic Functions I*, Princeton University, 1951.

[2] ———, *Geometric Algebra*, New York, 1957.

[3] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin, 1952.

[4] H. Hasse, "Symmetrische Matrizen im Körper der rationalen Zahlen," *Journal für die reine und angewandte Mathematik*, vol. 153 (1924), pp. 12-43.

[5] B. W. Jones, "A canonical quadratic form for the ring of 2-adic integers," *Duke Mathematical Journal*, vol. 11 (1944), pp. 715-727.

[6] ———, *The Arithmetic Theory of Quadratic Forms*, Carus Monographs, 1950.

[7] H. Minkowski, *Gesammelte Abhandlungen I*, Leipzig, 1911.

[8] O. T. O'Meara, "Quadratic forms over local fields," *American Journal of Mathematics*, vol. 77 (1955), pp. 87-116.

[9] ———, "Integral equivalence of quadratic forms in ramified local fields," *American Journal of Mathematics*, vol. 79 (1957), pp. 157-186.

[10] ———, "Local characterization of integral quadratic forms by Gauss sums," *American Jornal of Mathematics*, vol. 79 (1957), pp. 687-709.

[11] G. Pall, "The arithmetical invariants of quadratic forms," *Bulletin of the American Mathematical Society*, vol. 51 (1945), pp. 185-197.

[12] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern," *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), pp. 31-44.

ON POWER MULTIPLICATIVE NORMS.*

By SILVIO AURORA.

1. **Introduction.** In [4], A. Ostrowski classified the absolute values (for definitions, see section 2) of fields as either archimedean or non-archimedean, and showed that a field with an archimedean absolute value may be embedded in the complex field.

The key result of this paper occurs in seceion 4 and describes the structure of norms[1] (of rings) having the properties that $\| x^2 \| = \| x \|^2$ for all x, and $\| \cdots xy \cdots \| = \| \cdots yx \cdots \|$ for all x and y. Such norms are classified as archimedean or non-archimedean in section 5, and the archimedean case is further broken down into two cases: the strictly archimedean, and the partially archimedean. In section 6, Ostrowski's embedding theorem is generalized to show that division rings having an archimedean norm of this type are algebraically embeddable in the ring of quaternions. Also, a division ring with a non-discrete, strictly archimedean norm of this type is shown to be algebraically and topologically isomorphic to a subring of the ring of quaternions. Finally, section 7 outlines a description of all norms of the ring of integers or the field of rationals such that $\| x^2 \| = \| x \|^2$ for all x.

2. **Pseudonorms and pseudometric rings.** We shall consider in this paper associative rings which do not necessarily possess a unit element.

By a *pseudonorm* of a ring R is meant a real-valued function N defined on R and such that:

(i) $N(0) = 0$.

(ii) $N(x+y) \leqq N(x) + N(y)$ for all x and y in R.

(iii) $N(-x) = N(x)$ for all x in R.

(iv) $N(xy) \leqq N(x)N(y)$ for all x and y in R.

(We find it more convenient to use standard function notation, such as $N(x)$, rather than the usual notation for norms, such as $\| x \|$.) A pseudonorm N

---

* Received February 27, 1958.

[1] Many of the results are actually stated for the more general case of *pseudonorms*.

such that $N(x)=0$ only if $x=0$ is called a *norm*. If a pseudonorm (norm) N satisfies the condition: (iv′) $N(xy)=N(x)N(y)$ for all x and y in R, which is a stronger requirement than (iv), then N is called a *pseudo absolute value* (*absolute value*).

If N is a pseudonorm for a ring R, an element x of R is called *N-null* provided that $N(x)=0$; the set of N-null elements of R is a two-sided ideal $I(N)$, which we shall call the *null ideal* of N. It is clear that the function N is constant on each residue class modulo $I(N)$, so that the function $\bar{N}$ such that $\bar{N}(A)$ is the common value assumed by N on the elements of the residue class A is a natural norm for the ring $\bar{R}=R/I(N)$ of residue classes modulo $I(N)$. (Compare Bourbaki in Exercise 13 at the end of Chapter IX, § 3 of [3], where $\bar{N}$ is said to be "associated" with N.)

We now exhibit some examples of pseudonorms:

(1) The *zero pseudonorm*, Z, of any ring is defined to be identically zero on the ring. This is always a pseudo absolute value, and it is clear that a pseudonorm N coincides with Z if and only if $I(N)$ is the entire ring.

(2) The *trivial norm*, T, of any ring is defined to be identically 1 in value on the non-zero elements of that ring. This norm is an absolute value if and only if the ring has no proper zero-divisors.

(3) The *ordinary* absolute value, A, is defined by $A(x)=|x|$ for all x, on any subring of the ring of real quaternions.

(4) The *p-adic* absolute value, B_p, where p is a rational prime, is defined on any subring of the field of rational numbers by the condition $B_p(x)=p^{-r}$ if x is a non-zero rational number having a representation $x=p^r\cdot(m/n)$, with m and n non-zero integers relatively prime to p, and with r an integer.

(5) If Q is a compact Hausdorff space and $C(Q)$ is the ring of all continuous complex-valued functions on Q, then the *supremum norm* S, such that $S(x)=\sup\{|x(q)| \mid q \text{ in } Q\}$, is of course a norm for $C(Q)$, but is an absolute value only when Q reduces to a single point.

(6) If I is a two-sided ideal of the ring R, the function $T^{(I)}$ which is the characteristic function of the complement of I is clearly a pseudonorm. Also, $T^{(I)}$ is a norm if and only if I is the zero ideal, and $T^{(I)}$ is a pseudo absolute value if and only if I is such that xy in I implies x in I or y in I.

The function $d(x,y)=N(x-y)$ is a pseudometric (metric) for R if

N is a pseudonorm (norm) for R. Also, the pseudometric $d(x,y)$ induces in the usual way a topology in R relative to which the ring operations are continuous. A ring R, together with a pseudonorm (norm, absolute value) for R, is called a *pseudometric ring* (*metric ring, ring with absolute value*). Thus, a pseudometric ring is a topological ring in the weak sense of the term; that is, the topology is not necessarily Hausdorff. In particular, a metric ring is a topological ring in the usual sense, and any pseudometric ring may be "coagulated" into a metric ring by passing to the ring of residue classes modulo the null ideal, with the "associated" norm. Such concepts as fundamental sequences, completeness, etc., are introduced in the obvious way for metric rings, and the usual results about these concepts are easily established.

A topological ring R such that $R^2 \neq \{0\}$ will be called *simple* if the only closed two-sided ideals are $\{0\}$ and R. In particular, for a discrete ring, simplicity coincides with the usual, purely algebraic concept as defined in [1]. For a pseudometric ring, the null ideal is obviously a closed two-sided ideal; thus, the null ideal of a simple pseudometric ring is either $\{0\}$, in which case the pseudonorm is a norm, or is the whole ring, in which case the pseudonorm is Z. That is, a simple pseudometric ring is either a simple metric ring or has the zero pseudonorm. It is clear that a metric ring which is simple in the purely algebraic sense is a simple metric ring. However, the converse is not true, for the ring generated by π and the rational numbers, and having A as its norm, is a simple metric ring but is obviously not simple in the purely algebraic sense.

3. The semi-lattice of pseudonorms. In this section, we shall consider an ordering of the set $\mathfrak{N}_R$ of all pseudonorms of a ring R. If N and N' are pseudonorms for R, we say that N' is *subordinate* to N, and write $N' \leqq N$ (also $N \geqq N'$), provided that $N'(x) \leqq N(x)$ for all x in R. This relation is clearly a partial ordering of $\mathfrak{N}_R$. It may also be noted that if $N' \leqq N$, then $I(N) \subset I(N')$. However, the correspondence which assigns $I(N)$ to N is not one-to-one. For example, T is subordinate to A, but distinct from A, on the ring of integers, while $I(A) = I(T)$ since both ideals contain only 0.

A non-empty family $\{N_\lambda \mid \lambda \in \Lambda\}$ of pseudonorms of a ring R is said to be *bounded* if, for each x in R, the set $\{N_\lambda(x) \mid \lambda \in \Lambda\}$ is bounded. If $\{N_\lambda \mid \lambda \in \Lambda\}$ is a bounded family of pseudonorms of R, then the function N such that, for each x in R, $N(x) = \sup\{N_\lambda(x) \mid \lambda \in \Lambda\}$ is easily seen to be a pseudonorm on R; we shall call N the *join* of the family $\{N_\lambda \mid \lambda \in \Lambda\}$ and denote it by the symbol $\vee\{N_\lambda \mid \lambda \in \Lambda\}$. (For a finite family $\{N_1, \cdots, N_k\}$, we shall also denote the join by $N_1 \vee \cdots \vee N_k$.) In terms of the customary terminology for partially ordered sets, the bounded families of pseudonorms of R are precisely the subsets of $\mathfrak{N}_R$ which have upper bounds in $\mathfrak{N}_R$, and the join of a bounded family is its least upper bound in $\mathfrak{N}_R$. Since a finite family of pseudonorms of R is always bounded and consequently has a join in $\mathfrak{N}_R$, the system $\mathfrak{N}_R$ is an upper semi-lattice.

A pseudonorm N of a ring R will be called *stable* if $N(\cdots xy\cdots) = N(\cdots yx\cdots)$ for all x and y in R. Any pseudo absolute value is clearly stable, and all pseudonorms of a commutative ring are stable. However, if R is any ring having elements x and y such that $xy = 0$ but $yx \neq 0$, then $T(xy) = 0$ and $T(yx) = 1$, so T is not stable on such a ring; thus, there even exist norms which are not stable.

If a pseudonorm N of a ring R has the property that $N(x^2) = [N(x)]^2$ for all x in R, then N will be called a *power multiplicative* pseudonorm (or *PM* pseudonorm for brevity). It is easily seen that if N is a *PM* pseudonorm then $N(x^r) = [N(x)]^r$ for every x in R and every natural number r; it follows easily that $N(x^r \cdot x^s) = N(x^r)N(x^s)$ for any x in R when r and s are natural numbers. The latter property explains the choice of the term "power multiplicative" to describe such a pseudonorm. Any pseudo absolute value is a *PM* pseudonorm, and the supremum norm S (of example (5) above) is also clearly power multiplicative. Not all pseudonorms are power multiplicative, however, even if they are norms; for example, the functions $2A$ and $A + T$ are norms of the real field but are not power multiplicative.

It is easily shown that the join of stable pseudonorms is stable, and the join of *PM* pseudonorms is a *PM* pseudonorm. Since a pseudo absolute value is always a stable *PM* pseudonorm, it follows that the join of a bounded family of pseudo absolute values is a stable *PM* pseudonorm. The converse, that every stable *PM* pseudonorm is the join of a bounded family of pseudo absolute values, is also true and constitutes the fundamental theorem on stable *PM* pseudonorms. This theorem will be established in the following section.

4. The structure of stable *PM* pseudonorms. We shall first introduce a method for constructing from a given pseudonorm various other pseudonorms subordinate to it. Let N be a pseudonorm of a ring R, and let c be an element of R which is not N-null. For any x in R, we have the inequalities:

$$N(x) \geqq N(xc)/N(c) \geqq N(xc^2)/[N(c)]^2 \geqq \cdots \geqq 0.$$

Then for any x in R, there is defined a non-negative number $N_c(x) = \lim_{r\to\infty} N(xc^r)/[N(c)]^r$. If N is a stable pseudonorm of R, it is easily proved that N_c is a stable pseudonorm subordinate to N. We shall refer to N_c as *the subordinate pseudonorm of N induced by c*, or simply as an *induced pseudonorm* of N. In the present discussion, we are concerned mainly with power multiplicative pseudonorms; the lemma which follows gives some properties of the induced pseudonorms for this special case.

LEMMA 1. *Let N be a non-zero stable PM pseudonorm of a ring R, and let c be an element of R which is not N-null. Then N_c is a non-zero stable PM pseudonorm of R such that:* (i) *N_c is subordinate to N,* (ii) $N_c(c) = N(c)$, (iii) $N_c(cx) = N_c(c)N_c(x)$ *for all x in R.*

Proof. That N_c is a stable pseudonorm subordinate to N has already been noted. We have $N_c(c) = \lim_{r\to\infty} N(c^{r+1})/[N(c)]^r = \lim_{r\to\infty} [N(c)]^{r+1}/[N(c)]^r = N(c)$ since N is power multiplicative. This proves (ii) and also shows that N_c is non-zero, since $N_c(c) = N(c) \neq 0$. To prove (iii), we note that $N_c(cx) = \lim_{r\to\infty} N(c^{r+1}x)/[N(c)]^r = N(c) \lim_{r\to\infty} N(c^{r+1}x)/[N(c)]^{r+1} = N(c)N_c(x) = N_c(c)N_c(x)$ for any x. Finally, to show that N_c is power multiplicative, we note that $\{N_c(x)\}^2 = \{\lim_{r\to\infty} N(xc^r)/[N(c)]^r\}^2 = \lim_{r\to\infty} \{N(xc^r)/[N(c)]^r\}^2 = \lim_{r\to\infty} N(x^2c^{2r})/[N(c)]^{2r} = N_c(x^2)$ for any x.

A non-empty set $\mathfrak{N}$ of non-zero stable *PM* pseudonorms on a ring R will be called a *hereditary system* if $\mathfrak{N}$ contains all the induced pseduonorms of its members. The preceding lemma tells us that the set of all non-zero stable *PM* pseudonorms on a ring is hereditary if it is non-empty, and the set of all non-zero stable *PM* pseudonorms subordinate to a given non-zero stable *PM* pseudonorm is always hereditary.

LEMMA 2. *A minimal element of a hereditary system $\mathfrak{N}$ must be a non-zero pseudo absolute value.*

Proof. If N is a minimal element of $\mathfrak{N}$, then N is non-zero since all elements of $\mathfrak{N}$ are non-zero. If c and d are arbitrary elements of the ring involved, we have $N(cd) = N(c)N(d)$ if c is N-null, for both sides of the equation are then zero. If c is not N-null, then N_c is defined and belongs to $\mathfrak{N}$, with $N_c(cd) = N_c(c)N_c(d)$ by Lemma 1(iii). But $N_c \leqq N$, so $N = N_c$ since N is a minimal element of $\mathfrak{N}$; thus, $N(cd) = N(c)N(d)$ in this case also. This shows that N is a pseudo absolute value.

It should be noted that Lemma 2 describes the minimal elements of a hereditary system *if there are minimal elements in it.* The example which follows shows that a hereditary system need not have minimal elements. In the ring R of even integers, let $N^n(x) = [B_2(x)]^n$ for each x in R. Then $\mathfrak{N} = \{N^1, N^2, N^3, \cdots\}$ is a hereditary system and is simply ordered, with $N^1 \geqq N^2 \geqq N^3 \geqq \cdots$; also, $N^n(2) = 2^{-n}$ and $N^{n+1}(2) = 2^{-n-1}$, so $N^n \neq N^{n+1}$ for every natural number n, and it follows that $\mathfrak{N}$ has no minimal element. The same example shows that a pseudo absolute value in a hereditary system is not necessarily a minimal element of that system, for in this example, it is easily seen that every element of $\mathfrak{N}$ is actually an absolute value.

We shall now consider certain collections of pseudonorms on a ring R that form hereditary systems which always have minimal elements. If N is a non-zero stable *PM* pseudonorm on R, and if c is an element of R which is not N-null, let $[R; N; c]$ be the set of all stable *PM* pseudonorms N' on R such that: (i) N' is subordinate to N, (ii) $N'(c) = N(c)$, and (iii) $N'(cx) = N'(c)N'(x)$ for all x in R. Note that (ii) insures that the elements of $[R; N; c]$ are non-zero.

Lemma 3. *$[R; N; c]$ is a hereditary system.*

Proof. $[R; N; c]$ is not empty since Lemma 1 implies that it contains N_c. If N' is any member of $[R; N; c]$ and d is not N'-null, then N'_d is a non-zero stable *PM* pseudonorm by Lemma 1. Also, N'_d is subordinate to N' and hence to N. Next,

$$N'_d(c) = \lim_{r\to\infty} N'(cd^r)/[N'(d)]^r = \lim_{r\to\infty} N'(c)N'(d^r)/N'(d^r) = N'(c) = N(c)$$

since N' is power multiplicative and has properties (iii) and (ii) of a system $[R; N; c]$. Finally,

$$\begin{aligned} N'_d(cx) &= \lim_{r\to\infty} \{N'(cxd^r)/[N'(d)]^r\} \\ &= \lim_{r\to\infty} \{N'(c)N'(xd^r)/[N'(d)]^r\} = N'(c)N'_d(x) = N'_d(c)N'_d(x) \end{aligned}$$

for any x. Thus, N'_d is also in $[R; N; c]$ when N' is in $[R; N; c]$, and the set $[R; N; c]$ is therefore a hereditary system.

Lemma 4. *$[R; N; c]$ contains minimal elements.*

Proof. Let $\mathfrak{N}$ be any non-empty simply ordered subset of $[R; N; c]$. Let $N'(x) = \inf\{N_\alpha(x) \mid N_\alpha \in \mathfrak{N}\}$ for each x in R. It is easily verified that N' is a stable *PM* pseudonorm which satisfies (i), (ii) and (iii); thus, N' belongs to $[R; N; c]$. Clearly, N' is subordinate to every element of $\mathfrak{N}$. Thus, every non-empty simply ordered subset of $[R; N; c]$ has a lower bound in $[R; N; c]$. An application of Zorn's Lemma shows that $[R; N; c]$ contains minimal elements.

The preceding lemma shows that any system $[R;N;c]$ contains minimal elements, which are necessarily non-zero pseudo absolute values by Lemmas 2 and 3, and which are subordinate to N by the definition of $[R;N;c]$. If N is a pseudonorm of a ring R, and if c is an element of R which is not N-null, by a *component of* N *at* c we shall mean any pseudo absolute value N' subordinate to N and such that $N'(c)=N(c)$. (Thus, a component is always non-zero.) If N is a non-zero stable *PM* pseduonorm of a ring R and c is an element of R which is not N-null, then any component of N at c must obviously belong to $[R;N;c]$; on the other hand, the minimal elements of $[R;N;c]$ are clearly components of N at c, so there are always components of N at c when c is not N-null.

THEOREM 1. (Fundamental theorem) *If* N *is a non-zero stable PM pseudonorm on a ring* R, *then* N *is the join of a bounded family of pseudo absolute values on* R.

Proof. Let $\mathfrak{N}$ be the set of all minimal elements of the sets $[R;N;c]$ as c ranges over the elements of R which are not N-null. Then $\mathfrak{N}$ is non-empty by Lemma 4, and consists of components of N according to the discussion preceding this theorem. The elements of $\mathfrak{N}$ are all subordinate to N, so their join, N', is also subordinate to N.

If c is an N-null element of R, we have $N(c)=N'(c)=0$. If c is not N-null, then $[R;N;c]$ contains a minimal element N'' by Lemma 4, and $N''(c)=N(c)$ by definition of $[R;N;c]$; but since $N\geqq N'\geqq N''$, we must have $N(c)\geqq N'(c)\geqq N''(c)$, so $N(c)=N'(c)$. Thus, for any c in R, $N(c)=N'(c)$, whence $N=N'$. This proves that N is the join of the elements of $\mathfrak{N}$, which are components and, in particular, pseudo absolute values.

If $\mathfrak{N}'$ is any non-empty set of pseudo absolute values subordinate to N, then the join of $\mathfrak{N}'$ is clearly subordinate to N. On the other hand, if $\mathfrak{N}'$ is a bounded family of pseudo absolute values on R such that $\mathfrak{N}'\supset\mathfrak{N}$, then N, which is the join of $\mathfrak{N}$, is obviously subordinate to the join of $\mathfrak{N}'$. Thus, if $\mathfrak{N}'$ is a set of pseudo absolute values subordinate to N such that $\mathfrak{N}'\supset\mathfrak{N}$, then the join of $\mathfrak{N}'$ is precisely N. This hypothesis is clearly fulfilled if we take as $\mathfrak{N}'$ either the set of all components of N, or the set of all pseudo absolute values subordinate to N. We thus obtain the following corollaries.

COROLLARY 1. *A non-zero stable PM pseudonorm is the join of its set of components.*

COROLLARY 2. *A non-zero stable PM pseudonorm is the join of the set of all pseudo absolute values subordinate to it.*

It is also possible to describe the rings which admit non-zero stable *PM* pseudonorms.

COROLLARY 3. *In order that a ring R admit a non-zero stable PM pseudonorm, it is necessary and sufficient that there exist a two-sided ideal I contained properly in R and such that xy in I implies x in I or y in I.*

Proof. The sufficiency is seen by taking the pseudonorm $T^{(I)}$ of example (6) in section 2, for this pseudonorm is then a non-zero pseudo absolute value and therefore certainly a stable *PM* pseudonorm. To see the necessity, a non-zero stable *PM* pseudonorm has a non-zero component because of Corollary 1, and the null ideal of such a component may be taken as I.

An example of the representation of a stable *PM* pseudonorm in terms of pseudo absolute values is given by example (5) of section 2. For a fixed q in Q, let $S_q(x) = |x(q)|$ for all x in $C(Q)$. It is clear that S_q is a pseudo absolute value for each q, and that S_q is in fact a component of S. Clearly, $S = \bigvee \{S_q \mid q \in Q\}$, but the representation of S as the join of pseudo absolute values is not unique since we also have $S = \bigvee \{S_q \mid q \in E\}$ for any set E dense in Q.

In this example, it is also seen that even though the pseudonorm S is actually a norm, the representation of S is in terms of pseudo absolute values, but not absolute values. Indeed, $C(Q)$ admits no absolute values if Q has more than one point, for in this case $C(Q)$ clearly has proper zero-divisors, whereas a ring with absolute value obviously has no proper zero-divisors. However, for simple metric rings the representation of a stable *PM* norm can be shown to be in terms of absolute values.

For convenience, by a *PMN ring* we shall mean a metric ring having a stable *PM* norm. Also, terminology relating to the pseudonorm of a pseudometric ring will be applied to the ring itself. For example, by a "subordinate pseudonorm" of a pseudometric ring will be meant one subordinate to the pseudonorm of that ring.

LEMMA 5. *A subordinate pseudonorm of a pseudometric ring R is continuous on R.*

Proof. Let N be the pseudonorm of R, and let N' be a subordinate pseudonorm. The inequality $|N'(x) - N'(y)| \leqq N'(x-y) \leqq N(x-y)$ for all x and y in R implies that N' is continuous on R.

THEOREM 2. *Every non-zero subordinate pseudonorm (pseudo absolute value) of a simple metric ring is a norm (absolute value).*

Proof. By Lemma 5, a subordinate pseudonorm is continuous, so its null ideal is a closed two-sided ideal (different from the whole ring when the pseudonorm is non-zero). For a simple metric ring, it follows that the null-ideal of a non-zero subordinate pseudonorm N' is the zero ideal, whence N' is a norm. If N' was also a pseudo absolute value, then N' must be an absolute value.

If we apply this result to Corollaries 1 and 2 of Theorem 1, we may conclude that, for a simple metric ring having a stable *PM* norm, we have a representation of the norm in terms of absolute values.

COROLLARY 1. *The norm of a simple PMN ring is the join of its components, which are all absolute values.*

COROLLARY 2. *The norm of a simple PMN ring is the join of all the subordinate absolute values.*

5. The classification of stable *PM* pseudonorms.

In the sequel, all rings are assumed to possess a unit element, e. A pseudonorm N on a ring R will be called *non-archimedean* if $N(x+y) \leqq \max(N(x), N(y))$ for all x and y in R, and N will be called *archimedean* if it is not non-archimedean.

If N is a pseudonorm of a ring R, and if γ is a positive number, let $N^\gamma(x) = [N(x)]^\gamma$ for all x in R. It is clear that N^γ satisfies all the defining conditions of a pseudonorm, except possibly (ii). Also, if N^γ is a pseudonorm, then it is easily proved that N^δ is a pseudonorm whenever $0 < \delta < \gamma$. If we define N^0 by the conditions $N^0(x) = 0$ when $N(x) = 0$ and $N^0(x) = 1$ when $N(x) \neq 0$, then N^0 is always a pseudonorm. Thus, the set of non-negative numbers γ such that N^γ is a pseudonorm on R must be a finite closed interval $[0, \mu]$, with $\mu \geqq 1$, or the infinite interval $[0, +\infty[$. It is easily proved that the infinite interval occurs if and only if N is non-archimedean. (Compare the corresponding statement in Chap. IX, § 3, no. 2 of [3] for the case of absolute values of division rings.) However, this characterization of the non-archimedean pseudonorms does not seem to be useful way of determining whether a given pseudonorm is non-archimedean.

We shall give below some criteria for classifying stable *PM* pseudonorms as archimedean or non-archimedean. First, we note that if N is a non-zero *PM* pseudonorm, then e is not in $I(N)$, so $N(e) = 1$ since $N(e) = N(e^2) = [N(e)]^2$. For a non-archimedean *PM* pseudonorm N, it follows that

$N(ne) \leqq 1$ for every natural number n. Thus, a PM pseudonorm N must be archimedean if there exists a natural number n for which $N(ne) > 1$.

LEMMA 6. *Let N be a PM pseudonorm, and let m be an integer with $m > 1$. Then $N(ne) \leqq 1$ for every natural number n if and only if $N(me) \leqq 1$.*

Proof. The result is easily proved along standard lines, by writing n^r in terms of the base m, etc.

LEMMA 7. *Let N be a PM pseudonorm of a ring R, and let m be an integer with $m > 1$. Then $N(me) \leqq 1$ if and only if*

$$N(x+y) \leqq \max(N(x), N(y))$$

whenever x and y are elements of R which commute.

Proof. First, suppose $N(x+y) \leqq \max(N(x), N(y))$ whenever x and y commute. Since N is a PM pseudonorm, we have $N(e) \leqq 1$. Let k be the smallest natural number for which $N((k+1)e) > 1$. But ke and e commute whenver k is a natural number, so

$$N((k+1)e) = N(ke+e) \leqq \max(N(ke), N(e)) \leqq 1,$$

and this is a contradiction. It follows that we have $N(ne) \leqq 1$ for every natural number n, so we have $N(me) \leqq 1$.

Conversely, if $N(me) \leqq 1$, then Lemma 6 implies that $N(ne) \leqq 1$ for every natural number n. If x and y commute, we have $(x+y)^r = \sum C^r{}_k x^k y^{r-k}$, so

$$\begin{aligned}[N(x+y)]^r = N((x+y)^r) &= N(\sum C^r{}_k x^k y^{r-k}) \leqq \sum N(C^r{}_k \cdot e) N(x)^k N(y)^{r-k} \\ &\leqq \sum N(x)^k N(y)^{r-k} \leqq (r+1)[\max(N(x), N(y))]^r.\end{aligned}$$

By extracting r-th roots of the end terms and letting r become infinite, we obtain $N(x+y) \leqq \max(N(x), N(y))$.

THEOREM 3. *Let N be a PM pseudonorm of a commutative ring R, and let m be an integer with $m > 1$. Then N is non-archimedean if and only if $N(me) \leqq 1$.*

Proof. This follows obviously from Lemma 7.

COROLLARY. *Let N and N' be PM pseudonorms of a commutative ring R such that $N' \leqq N$. If N is non-archimedean, then N' is non-archimedean.*

LEMMA 8. *The join of a bounded family of non-archimedean pseudonorms on a ring R is a non-archimedean pseudonorm on R.*

COROLLARY. *A commutative PMN ring is non-archimedean if and only if every subordinate pseudo absolute value is non-archimedean.*

LEMMA 9. *If N is an absolute value for a division ring R and m is an integer with $m > 1$, then N is non-archimedean if and only if $N(me) \leqq 1$.*

Proof. If N is non-archimedean, we obviously have $N(me) \leqq 1$. Conversely, if $N(me) \leqq 1$ we apply Lemma 7, so that

$$\begin{aligned} N(x+y) &= N(x)N(e+x^{-1}) \leqq N(x)\max(N(e), N(x^{-1}y)) \\ &= \max(N(x), N(y)) \end{aligned}$$

if $x \neq 0$, since e and $x^{-1}y$ commute.

THEOREM 4. *If N is a stable PM norm for a division ring R and m is an integer with $m > 1$, then N is non-archimedean if and only if $N(me) \leqq 1$.*

Proof. If $N(me) \leqq 1$, then $N'(me) \leqq 1$ for any absolute value N' subordinate to N, so N' is non-archimedean by Lemma 9. But N is the join of all absolute values subordinate to it, according to Corollary 2 of Theorem 2, and these are all non-archimedean; so N is non-archimedean by Lemma 8. The remainder of the theorem is obvious.

COROLLARY 1. *Every subordinate stable PM norm of non-archimedean PMN division ring is non-archimedean.*

COROLLARY 2. *If $\{N_\lambda \mid \lambda \in \Lambda\}$ is a bounded family of stable PM norms of a division ring R, then $\bigvee\{N_\lambda \mid \lambda \in \Lambda\}$ is non-archimedean on R if and only if N_λ is non-archimedean for each λ in Λ.*

COROLLARY 3. *A stable PM norm N on a division ring is non-archimedean if and only if every absolute value subordinate to N is non-archimedean.*

Corollary 2 of Theorem 4, Lemma 8 and its corollary indicate that if a stable *PM* norm of a commutative ring or a division ring is expressed as the join of a family of pseudo absolute values, then the norm is non-archimedean if and only if every member of the family is non-archimedean. For an arbitrary ring, it may also be shown that a non-archimedean stable *PM* pseudonorm may always be expressed as the join of a bounded family of non-archimedean pseudo absolute values. (This is done by observing that the induced pseudonorms of a non-archimedean stable *PM* pseudonorm are also non-archimedean; the proof of the Fundamental Theorem is then paralleled, but with the sets $[R;N;c]$ now restricted to their non-archimedean members.)

If an archimedean stable *PM* pseudonorm is expressed as the join of a family of pseudo absolute values, Lemma 8 implies that they are not all non-archimedean. There are then two possibilities: either all of these pseudo absolute values are archimedean, or at least one is non-archimedean. An archimedean stable *PM* pseudonorm will be called *strictly archimedean* if it may be expressed in at least one way as the join of archimedean pseudo absolute values; otherwise it will be called *partially archimedean.*

THEOREM 5. *If N is a partially archimedean stable PM pseudonorm of a ring R, then there exist non-zero stable PM pseudonorms N' and N'' such that N' is strictly archimedean on R, N'' is non-archimedean on R, and $N = N' \vee N''$.*

Proof. N is expressed as the join of a family of pseudo absolute values on R. Then N' and N'' are defined as the join of the archimedean members of the family, and the join of the non-archimedean members of the family, respectively.

The set of stable *PM* pseudonorms on a ring is thus divided into three classes: the non-archimedean, the strictly archimedean, and the partially archimedean. The partially archimedean pseudonorms resemble the strictly archimedean ones in some respects, and resemble the non-archimedean pseudonorms in other respects; Theorem 5 suggests this situation since it shows that a partially archimedean pseudonorm is obtained by joining a strictly archimedean and a non-archimedean pseudonorm. In the theorem which follows, the resemblance of partially archimedean pseudonorms to the non-archimedean ones is in evidence. The corollaries and the following theorem then give sufficient conditions for *PMN* division rings to be strictly archimedean.

LEMMA 10. *If a metric ring R admits a non-archimedean subordinate norm N', then R is totally disconnected.*

Proof. N' is continuous by Lemma 5, so for any positive ϵ the set $\mathfrak{S}(\epsilon) = \{x \mid N'(x) < \epsilon\}$ is an open set of R. Since N' is non-archimedean, it follows easily that $\mathfrak{S}(\epsilon)$ is an additive group for each positive ϵ, so $\mathfrak{S}(\epsilon)$ is open and closed in R. The intersection of all the $\mathfrak{S}(\epsilon)$ as ϵ ranges over the positive numbers is clearly 0. Since 0 is the intersection of a family of sets which are both open and closed, the connected component of 0 consists only of 0. This shows that R is totally disconnected.

THEOREM 6. *Let R be a non-archimedean metric ring or a partially archimedean simple PMN ring. Then R is totally disconnected.*

Proof. If R is a non-archimedean metric ring with norm N, let $N' = N$ and apply Lemma 10. If R is a partially archimedean simple *PMN* ring with norm N, then Theorem 5 states that there is a non-zero non-archimedean pseudonorm N'' subordinate to N. Since R is simple, N'' is a norm, according to Theorem 2. The application of Lemma 10 to N'' shows that R is totally disconnected in this case also.

COROLLARY 1. *If a simple PMN ring R is not totally disconnected, then R is strictly archimedean.*

COROLLARY 2. *Every connected PMN division ring is strictly archimedean.*

THEOREM 7. *Let R be a PMN division ring with norm N, and let m be an integer with $m > 1$. If $me \neq 0$ and $N((me)^{-1}) < 1$, then R is strictly archimedean.*

Proof. Since $N((me)^{-1}) < 1$, we have $N'((me)^{-1}) < 1$ for N' a component of N. But $N'(me)N'((me)^{-1}) = 1$, so $N'(me) > 1$, and Theorem 4 implies that N' is archimedean. Thus, all components of N are archimedean, and N is the join of its components, by Corollary 1 of Theorem 2, so that N is strictly archimedean.

6. Embedding theorems for archimedean division rings.

A. Ostrowski showed in [4] that the archimedean fields with absolute value were algebraically and topologically isomorphic to subfields of the complex field. In this section, we shall generalize this result by showing that the archimedean *PMN* division rings are alegbraically isomorphic to division subrings of the division ring $\mathfrak{Q}$ of all real quaternions. In particular, the non-discrete, strictly archimedean *PMN* division rings will be shown to be algebraically and topologically isomorphic to division subrings of $\mathfrak{Q}$.

LEMMA 11. *If R is an archimedean division ring with absolute value, then R is algebraically and topologically isomorphic to a division subring of $\mathfrak{Q}$, and the norm in R corresponds to the ρ-th power of A, for some ρ such that $0 < \rho \leqq 1$.*

Proof. This follows from Theorem 11 of [2] and the statement following the corollary of that theorem.

THEOREM 8. *If R is an archimedean PMN division ring, then R is algebraically isomorphic to a division subring of* $\mathfrak{Q}$.

Proof. If N is the norm of R, then Corollary 1 of Theorem 2 states that N is the join of its components, which are all absolute values. Then Lemma 8 implies that the components are not all non-archimedean, for otherwise N would be non-archimedean. Let N' be an archimedean component of N, and apply Lemma 11 to R with N' taken as its norm. Then R is algebraically isomorphic to a division subring of $\mathfrak{Q}$.

LEMMA 12. *Let N be a non-zero pseudonorm of a ring R, and let Γ be a non-empty, bounded set of non-negative numbers such that N^{γ} is a pseudonorm for each γ in Γ. If $\alpha = \inf \Gamma$ and $\beta = \sup \Gamma$, then $\bigvee\{N^{\gamma} \mid \gamma \in \Gamma\} = N^{\alpha} \vee N^{\beta}$.*

Proof. The proof is elementary.

LEMMA 13. *Let R be a division subring of $\mathfrak{Q}$, and let N be a strictly archimedean stable PM norm on R. Then there exist real numbers α and β, with $0 < \alpha \leqq \beta \leqq 1$ or $0 = \alpha < \beta \leqq 1$, such that $N = A^{\alpha} \vee A^{\beta}$.*

Proof. Any archimedean absolute value on R must be of the form A^{γ} for some γ such that $0 < \gamma \leqq 1$. This follows from Lemma 11. But a strictly archimedean stable *PM* norm on a division ring is the join of a non-empty family of archimedean absolute values, so $N = \bigvee\{A^{\gamma} \mid \gamma \in \Gamma\}$, where Γ is a non-empty subset of $]0,1]$. Then Lemma 12 implies that $N = A^{\alpha} \vee A^{\beta}$, with $\alpha = \inf \Gamma$ and $\beta = \sup \Gamma$. Clearly, $0 \leqq \alpha \leqq \beta \leqq 1$, and β is positive. This completes the proof.

THEOREM 9. *Let R be a strictly archimedean, non-discrete PMN division ring. Then R is algebraically and topologically isomorphic to a division subring of Q.*

Proof. By Theorem 8, R is algebraically isomorphic to a division subring of $\mathfrak{Q}$. If we choose a specific algebraic isomorphism, we may consider R as a subset of $\mathfrak{Q}$. Lemma 13 shows that the norm of R is of the form $A^{\alpha} \vee A^{\beta}$, with $0 \leqq \alpha \leqq \beta \leqq 1$. Since R is not discrete, we must have α positive, for the norm $A^{0} \vee A^{\beta} = T \vee A^{\beta}$ is clearly discrete. Then $A^{\alpha} \vee A^{\beta}$, A^{α}, and A give the same topology on R, and so the topology given to R by its norm is the same as the relative topology of R considered as a subset of $\mathfrak{Q}$. Thus, the algebraic isomorphism of R into $\mathfrak{Q}$ is also a topological isomorphism (homeomorphism).

COROLLARY 1. *Let R be a strictly archimedean, non-discrete, complete PMN division ring. Then R is algebraically and topologically isomorphic to the real field $\mathfrak{R}$, the complex field $\mathfrak{C}$, or $\mathfrak{Q}$.*

COROLLARY 2. *Let R be a connected PMN division ring. Then R is algebraically and topologically isomorphic to a division subring of $\mathfrak{Q}$.*

COROLLARY 3. *Let R be a connected, complete PMN division ring. Then R is algebraically and topologically isomorphic to $\mathfrak{R}$, to $\mathfrak{C}$, or to $\mathfrak{Q}$.*

7. *PM* pseudonorms for special cases. In this section, we shall describe all non-zero *PM* pseudonorms of the rational field or of the ring of integers.

It is well known (see, for instance, chapter X of [5]) that the only absolute values of either of these rings are T, A^{γ} with $0 < \gamma \leqq 1$, and $B_p{}^{\gamma}$ with p a prime number and $\gamma > 0$. Also, it is easily proved that the only other non-zero pseudo absolute values of the ring of integers are of the type T_p, with p prime, where T_p is the characteristic function of the set of integers not divisible by p. Theorem 1 indicates that all non-zero *PM* pseudonorms of the ring of integers may be obtained by taking joins of pseudo absolute values of these four types, while Theorems 1 and 2 indicate that a *PM* norm of the rational field is the join of absolute values of the first three types. By the use of Lemma 12, these expressions may be simplified so that at most two powers of a given pseudo absolute value appear. Further simplifications may be made by the use of simple manipulations. It will suffice to describe the strictly archimedean and the non-zero non-archimedean cases, for the partially archimedean case is then easily described by using Theorem 5.

THEOREM 10. *Let N be a strictly archimedean PM norm of the rational field. Then either $N = A^{\alpha} \vee A^{\beta}$, with $0 < \alpha \leqq \beta \leqq 1$, or $N = T \vee A^{\beta}$, with $0 < \beta \leqq 1$.*

THEOREM 11. *Let N be a non-archimedean PM norm of the rational field. Then $N = T$, or $N = \bigvee \{B_p{}^{\alpha(p)} \vee B_p{}^{\beta(p)} \mid p \in \mathfrak{P}\}$ with $\mathfrak{P}$ a finite non-empty set of primes and $0 < \alpha(p) \leqq \beta(p)$ for all p in $\mathfrak{P}$, or*

$$N = T \vee [\bigvee \{B_p{}^{\beta(p)} \mid p \in \mathfrak{P}\}]$$

with $\mathfrak{P}$ a finite non-empty set of primes and $0 < \beta(p)$ for all p in $\mathfrak{P}$, or $N = \bigvee \{B_p{}^{\beta(p)} \mid p \in \mathfrak{P}\}$ with $\mathfrak{P}$ an infinite set of primes and $0 < \beta(p)$ for all p in $\mathfrak{P}$.

THEOREM 12. *Let N be a strictly archimedean PM pseudonorm on the ring of integers. Then $N = A^{\beta}$, with $0 < \beta \leqq 1$.*

THEOREM 13. *Let N be a non-zero non-archimedean PM pseudonorm of the ring of integers. Then $N = T$, or*

$$N = [\vee \{B_p{}^{\alpha(p)} \mid p \in \mathfrak{P}\}] \vee [\vee \{T_p \mid p \in \mathfrak{P}'\}],$$

where $\mathfrak{P}$ and $\mathfrak{P}'$ are disjoint finite sets of primes, not both empty, and $0 < \alpha(p)$ for all p in $\mathfrak{P}$.

NEW YORK CITY.

REFERENCES.

[1] E. Artin, C. J. Nesbitt and R. M. Thrall, *Rings with minimum condition*, Ann Arbor, 1944.

[2] S. Aurora, "Multiplicative norms for metric rings," *Pacific Journal of Mathematics*, vol. 7 (1957), pp. 1279-1304.

[3] N. Bourbaki, *Éléments de mathématique*, Livre III. *Topologie Générale*, Chapitres III, IX. Actualités Scientifiques et Industrielles, nos. 916, 1045; Paris, 1942-1948.

[4] A. Ostrowski, "Über einige Lösungen der Funktionalgleichung $\phi(x)\phi(y) = \phi(xy)$," *Acta Mathematica*, vol. 4 (1918), pp. 271-284.

[5] B. L. van der Waerden, *Modern algebra*, vol. 1, New York, 1953.

THE SUSPENSION OF A LOOP SPACE.*

By W. D. Barcus and J.-P. Meyer.[1]

Part I. The Homology Suspension.

1. Introduction. If X is a topological space, let SX denote the suspension of X, i. e., the join of X with a pair of points p_+, p_-, and let $\Omega(X, x_0)$ denote the space of loops on X at x_0. If Y is another space, let $M(Y, X)$ denote the set of all (continuous) maps $Y \to X$, and similarly for pairs and triples. There is a well-known 1-1 correspondence

$$\psi\colon M((SY, p_+, p_-), (X, x_0, x_0)) \to M(Y, \Omega(X, x_0)).$$

Let $i\colon SX \to \mathcal{S}X$ be the identification map, where $\mathcal{S}X$ is the reduced suspension. G. W. Whitehead [17] studied the homotopy suspension E: $\pi_n(X) \to \pi_{n+1}(SX)$ by using the map $\psi(i)\colon X \to \Omega\mathcal{S}X$. We consider a dual situation: abbreviate $\Omega(X, x_0)$ by Ω, and let $j\colon \Omega \to \Omega$ be the identity. Then the map $\psi^{-1}(j)\colon S\Omega \to X$ induces homomorphisms of the homology groups which are closely related to the homology suspension $\sigma\colon H_n(\Omega) \to H_{n+1}(X)$. It is convenient to convert $\psi^{-1}(j)$ into an equivalent fibre map. The fibre is of the homotopy type of the join $\Omega * \Omega$, and the Serre homology sequence of the fibering is essentially the same as G. W. Whitehead's sequence [18] involving σ, but contains an extra term. This gives an alternative proof of Whitehead's main result, and also allows us to extend several of his corollaries by one dimension: e. g. a cohomology operation of type $(n, q; \pi, G)$, $q \leqq 3n$, is additive if and only if it is a suspension. As a further application, in Part II we apply the above fibering to the problem of calculating the Postnikov invariants of the suspension of an Eilenberg-MacLane space $K(\pi, n)$.

2. Preliminaries. The homology theory used in this paper is the cubical singular theory of Serre [14] as modified by Bott and Samelson [3].

The Suspension. Let I be the unit interval. The suspension of X, SX,

---

* Received January 28, 1958.

[1] The work of Meyer was supported by ONR Contract Nonr-562(18), NR-043-176.

may be defined as the space obtained from $X \times I$ by the identifications $(x,0) = (x',0)$ and $(x,1) = (x',1)$ for all $x, x' \in X$. Let $\eta\colon X \times I \to SX$ be the identification map; we shall write the point $\eta(x,t)$ as $[x,t]$ and set $p_- = [x,0], p_+ = [x,1]$. The point p_- will usually be taken as a base-point. SX contains subspaces X_+, X, X_- which are, respectively, $\eta(X \times \{t \mid \frac{1}{2} \leqq t \leqq 1\})$, $\eta(X \times \frac{1}{2})$, and $\eta(X \times \{t \mid 0 \leqq t \leqq \frac{1}{2}\})$. The *suspension* $E\colon H_n(X) \to H_{n+1}(SX)$, not to be confused with the homology suspension (defined below), is the composition $j_*^{-1} i_* \partial^{-1}$:

$$\begin{tikzcd} H_n(X) & H_{n+1}(X_+, X) \arrow[l, "\partial"'] \arrow[r, "i_*"] & H_{n+1}(SX, X_-) & H_{n+1}(SX) \arrow[l, "j_*"'] \end{tikzcd} \qquad (n > 0).$$

We give a direct description of E. For a singular cube $f \in C_n(X)$, define $Sf \in C_{n+1}(SX)$ by

$$(2.1) \qquad Sf(t_1, \cdots, t_{n+1}) = [f(t_1, \cdots, t_n), t_{n+1}].$$

S commutes with the boundary operator for $n > 0$, and hence defines a homomorphism of the homology groups, still denoted by S.

(2.2) PROPOSITION. $E = (-1)^{n+1} S\colon H_n(X) \to H_{n+1}(SX) \quad (n > 0)$.

The proof is elementary, and is omitted.

The Homology Suspension. Let $(X; A, B)$ be a triad. Following Serre [14], we denote by $E_{A,B}(X)$ the space of (continuous) paths in X, starting in A and ending in B. If $x_0 \in X$, we abbreviate $E_{x_0,x_0}(X)$ by $\Omega(X, x_0)$. The map $p\colon E_{x_0,X}(X) \to X$ which assigns to each path its endpoint is a fibre map, the total space is contractible, and $p^{-1}(A) = E_{x_0,A}(X)$. The homomorphism

$$H_n(E_{x_0,A}(X)) \xrightarrow{\partial^{-1}} H_{n+1}(E_{x_0,X}(X), E_{x_0,A}(X)) \xrightarrow{p_*} H_{n+1}(X, A) \qquad (n > 0)$$

is well-defined, and is denoted by σ_A; σ_{x_0} is abbreviated by σ, and is called the *homology suspension.* Similarly, the map $p^{\#}\colon E_{X,x_0}(X) \to X$ which assigns to each path its initial point is a fibre map; the homomorphism corresponding to σ_A will be denoted $\sigma_A{}^{\#}\colon H_n(E_{A,x_0}(X)) \to H_{n+1}(X, A)$. By a slight modification of the argument on p. 482 of [14], one verifies that $(-1)^n \sigma_A$ is induced by a homomorphism $s\colon C_n(E_{x_0,A}(X)) \to C_{n+1}(X, A)$ defined on singular cubes by

$$(2.3) \qquad sf(t_1, \cdots, t_{n+1}) = f(t_1, \cdots, t_n)(t_{n+1}).$$

(2.4) PROPOSITION. *If (X, A) is q-connected and X is r-connected, then σ_A is an isomorphism for $0 < n < q + r$. A similar result hold for $\sigma_A{}^{\#}$.*

Proof. The fibre is $\Omega(X, x_0)$, which is $(r-1)$-connected. The result then follows from Theorem 1B, p. 268 of [15].

The Fundamental Map. For the remainder of Part I, X will denote a fixed topological space, $x_0 \in X$ a base-point possessing a contractible neighborhood in X, and $\Omega(X, x_0)$ will be abbreviated by Ω.

The *fundamental map* $k\colon S\Omega \to X$ is defined by $k[\omega, t] = \omega(t)$, $\omega \in \Omega$.

(2.5) PROPOSITION. $k_* E = -\sigma\colon H_n(\Omega) \to H_{n+1}(X)$.

Proof. Let $f \in C_n(\Omega)$ be a singular cube. Then

$$\begin{aligned} k(Sf)(t_1, \cdots, t_{n+1}) &= k[f(t_1, \cdots, t_n), t_{n+1}] = f(t_1, \cdots, t_n)(t_{n+1}) \\ &= sf(t_1, \cdots, t_{n+1}). \end{aligned}$$

Hence $(-1)^{n+1} k_* E = k_* S = (-1)^n \sigma$.

Homotopy Properties. There are well-known analogues of E and σ in homotopy; we recall briefly their definitions.

Let $x_0 \in \Omega$ denote the constant loop at $x_0 \in X$. Let $\alpha \in \pi_n(\Omega, x_0)$ be represented by $f\colon (I^n, \dot{I}^n) \to (\Omega, x_0)$; then $(-1)^n \sigma(\alpha) \in \pi_{n+1}(X, x_0)$ is represented by $f'\colon (I^{n+1}, \dot{I}^{n+1}) \to (X, x_0)$, where

$$f'(t_1, \cdots, t_{n+1}) = f(t_1, \cdots, t_n)(t_{n+1}).$$

By exactness, the injection $i_*\colon \pi_{n+1}(SX, p_-) \to \pi_{n+1}(SX, Sx_0)$ is an isomorphism for all n. If $\beta \in \pi_n(X, x_0)$ is represented by $g\colon (I^n, \dot{I}^n) \to (X, x_0)$, then $(-1)^{n+1} E\beta = i_*^{-1}\gamma$, where γ is the class of $g'\colon (I^{n+1}, \dot{I}^{n+1}) \to (SX, Sx_0)$, defined by

$$g'(t_1, \cdots, t_{n+1}) = [g(t_1, \cdots, t_n), t_{n+1}].$$

(2.6) PROPOSITION. $k_* E = -\sigma\colon \pi_n(\Omega, x_0) \to \pi_{n+1}(X, x_0)$.

The proof is similar to that in homology.

From (2.6) and the fact that σ is an isomorphism, we conclude

(2.7) COROLLARY. $k_*\colon \pi_{n+1}(S\Omega, p_-) \to \pi_{n+1}(X, x_0)$ *is an epimorphism, and* $E\colon \pi_n(\Omega, x_0) \to \pi_{n+1}(S\Omega, p_-)$ *is a monomorphism.*

Converting a Map into a Fibre Map. The following construction is due to Cartan and Serre [5]. Let $f\colon Y \to X$ be a map, and let M be the mapping cylinder of f: i.e. the space obtained from the disjoint union $Y \times I \cup X$ by identifying $(y, 1) = f(y) \in X$ for all $y \in Y$. Y and X are embedded in M as the images of the sets $Y \times 0$ and X respectively. The image in M of $(y, t) \in Y \times I$ will again be denoted by (y, t). Define $p\colon E_{Y,M}(M) \to M$ by

$p(\tau)=\tau(1)$; then p is a fibre map, and is equivalent to f in the following sense. Consider the diagram

(2.8)
$$\begin{tikzcd}
E_{Y,M}(M) \arrow[r, "p"] \arrow[d, shift left, "q"] & M \arrow[d, shift left, "r"] \\
Y \arrow[r, "f"] \arrow[u, shift left, "j"] & X \arrow[u, shift left, "l"]
\end{tikzcd}$$

where $j(y)$ is the constant path at y; $q(\tau)=\tau(0)$; l is the inclusion; and r is the retraction $r(y,t)=f(y)$, $r(x)=x$. Then qj and rl are equal to the appropriate identity maps, jq and lr are homotopic to the identities, and $rpj=f$.

If $f\colon Y\to X$ is an inclusion, we need not introduce the mapping cylinder: in this case we replace M by X and $l=r=$ identity.

3. The fibre space. In this and the next section, we study the fundamental map $k\colon S\Omega\to X$ by converting it into the fibre map $p\colon E_{S\Omega,M}(M)\to M$ described in § 2. As a base-point in M, we take $x_0\in X$; then the fibre over x_0 is $F=E_{S\Omega,x_0}(M)$.

The join $\Omega*\Omega$ is defined to be the space obtained from $\Omega\times I\times\Omega$ by identifying $(\mu,0,\nu)=(\mu,0,\nu')$ and $(\mu,1,\nu)=(\mu',1,\nu)$ for all $\mu,\mu',\nu,\nu'\in\Omega$. The point of $\Omega*\Omega$ which is the image of (μ,t,ν) will again be denoted (μ,t,ν). We define a function $h\colon\Omega*\Omega\to F$ as follows. If $y\in S\Omega$, let $\lambda(y)$ be the path in M from y to $k(y)\in X$ given by $\lambda(y)(s)=(y,s)$. If $\mu\in\Omega$ and $0\leqq a\leqq b\leqq 1$, we define the path $\mu_{a,b}$ from $\mu(a)$ to $\mu(b)$ by $\mu_{a,b}(s)=\mu((b-a)s+a)$. The inverse of $\mu_{a,b}$ will be denoted by $\mu_{a,b}{}^{-1}$. Then if $(\mu,t,\nu)\in\Omega*\Omega$,

$$h(\mu,t,\nu)=\begin{cases}\lambda[\mu\nu,t]\mu_{2t,1} & \text{if } 0\leqq t\leqq\frac{1}{2}\\ \lambda[\mu\nu,t]\nu_{0,2t-1}{}^{-1} & \text{if } \frac{1}{2}\leqq t\leqq 1.\end{cases}\tag{3.1}$$

(3.2) PROPOSITION. *The function h is well-defined and continuous. Furthermore, h is a homotopy equivalence, so that F is of the homotopy type of $\Omega*\Omega$.*

The proof is given in the appendix.

4. The homology sequence. Let $p\colon E\to B$ be a fibre space in which B is q-connected, $q\geqq 1$, and the fibre F is r-connected. Then by Corollary 1, p. 469 of [14], $p_*\colon H_i(E,F)\to H_i(B,b_0)$ is an isomorphism for $i\leqq q+r+1$, and an epimorphism for $i=q+r+2$, provided the coefficients are in a principal ideal ring Γ. According to Lemma 5.2 of [18], the same result therefore holds with coefficients in any Γ-module A. From the homology sequence of the pair (E,F) with coefficients in A, we thus derive the exact Serre sequence of the fibering ([14], p. 468) with coefficients in A:

$$H_{q+r+1}(F) \xrightarrow{i_*} H_{q+r+1}(E) \xrightarrow{p_*} H_{q+r+1}(B) \xrightarrow{\tau} H_{q+r}(F) \rightarrow \cdots.$$

Here i_* denotes the injection and τ the transgression.

Throughout the remainder of this section, all homology groups are to have coefficients in a fixed Abelian group G.

Let X be n-connected, $n \geqq 1$. Then $\Omega * \Omega$ is $2n$-connected, and the Serre sequence of the fibering of § 3 is (using the above remarks with Γ the ring of integers, $A = G$)

$$H_{3n+1}(F) \xrightarrow{i_*} H_{3n+1}(E_{S\Omega,M}(M)) \xrightarrow{p_*} H_{3n+1}(M) \xrightarrow{\tau} \cdots. \tag{4.1}$$

In this section, we shall give alternative expressions for the homomorphisms in (4.1).

Recall that Lemma (2.5) of [18] states that there is a unique homomorphism ρ such that the following diagram is commutative for $i \geqq 1$, where $\Omega \vee \Omega = \Omega \times x_0 \cup x_0 \times \Omega$, j' is the inclusion, m is the multiplication in Ω, $p_1, p_2\colon \Omega \times \Omega \rightarrow \Omega$ are the projections, and $\xi = m_* - p_{1*} - p_{2*}$:

$$\begin{tikzcd}
H_i(\Omega \times \Omega) \arrow[rr, "j'_*"] \arrow[dr, "\xi"'] & & H_i(\Omega \times \Omega, \Omega \vee \Omega) \arrow[dl, "\rho"] \\
& H_i(\Omega) &
\end{tikzcd}$$

(4.2) PROPOSITION. *There exists a commutative diagram for $i > 1$, in which θ_1, θ_2 and r_* are isomorphisms:*

$$\begin{tikzcd}
H_i(F) \arrow[r, "i_*"] \arrow[d, "\theta_1"] & H_i(E_{S\Omega,M}(M)) \arrow[r, "p_*"] \arrow[d, "\theta_2"] & H_i(M) \arrow[d, "r_*"] \\
H_{i-1}(\Omega \times \Omega, \Omega \vee \Omega) \arrow[r, "\rho"] & H_{i-1}(\Omega) \arrow[r, "\sigma"] & H_i(X)
\end{tikzcd} \tag{4.3}$$

Proof. Consider the second square, in which $\theta_2 = -E^{-1}q_*$; q and r are defined in diagram (2.8). According to the remarks following (2.8), with $f = k$, we have $k_*q_* = r_*p_*$; hence, using (2.5),

$$\sigma\theta_2 = -\sigma E^{-1}q_* = k_*q_* = r_*p_*.$$

Since q and r are homotopy equivalences, q_* and r_* are isomorphisms. E is an isomorphism, and hence so is θ_2.

To prove commutativity in the first square, we consider the following diagram, in which $\phi\colon \Omega * \Omega \to S(\Omega \times \Omega)$ is defined by $\phi(\mu, t, \nu) = [(\mu, \nu), t]$, Sm is the suspension of m, and $S\xi = (Sm)_* - (Sp_1)_* - (Sp_2)_*$:

(4.4)

$$\begin{tikzcd}
 & H_i(F) \arrow[rr, "i_*"] & & H_i(E_{S\Omega,M}(M)) \arrow[dd, "q_*"] \\
 & H_i(\Omega * \Omega) \arrow[u, "h_*"] \arrow[d, "\phi_*"] & & \\
H_i(S(\Omega \times \Omega), S(\Omega \vee \Omega)) & H_i(S(\Omega \times \Omega)) \arrow[l, "j''_*"'] \arrow[rr, "S\xi"] & & H_i(S\Omega) \\
 & H_{i-1}(\Omega \times \Omega) \arrow[u, "E"] \arrow[rr, "\xi"] \arrow[d, "j'_*"] & & H_{i-1}(\Omega) \arrow[u, "E"'] \\
 & H_{i-1}(\Omega \times \Omega, \Omega \vee \Omega) \arrow[uul, "E"] \arrow[urr, "\rho"'] & &
\end{tikzcd}$$

$$\text{Now}\quad qih(\mu, t, \nu) = \begin{cases} q(\lambda[\mu\nu, t]\mu_{2t,1}) & \text{if } 0 \leqq t \leqq \frac{1}{2} \\ g(\lambda[\mu\nu, t]\nu_{0,2t-1^{-1}}) & \text{if } \frac{1}{2} \leqq t \leqq 1 \end{cases}$$
$$= [\mu\nu, t];$$

also, $Sm\phi(\mu, t, \nu) = [\mu\nu, t]$;

hence $q_*i_*h_* = (Sm)_*\phi_* = S\xi\phi_*$, since $(Sp_1)_*\phi_* = (Sp_2)_*\phi_* = 0$, and the top rectangle of (4.4) is commutative. The remainder of the diagram is obviously commutative.

One deduces immediately from the proof of Lemma (7.2) in [19] that $j''_*\phi_*$ is an isomorphism; hence so are $E^{-1}j''_*\phi_* = j'_*E^{-1}\phi_*$ and $\theta_1 = -j'_*E^{-1}\phi_*h_*^{-1}$. Since $\theta_2 = -E^{-1}q_*$, commutativity of (4.4) implies that $\rho\theta_1 = \theta_2 i_*$. This completes the proof of (4.2).

Henceforth, we shall set $S\Omega \vee S\Omega = S\Omega \times p_- \cup p_+ \times S\Omega \subset S\Omega \times S\Omega$, and $M \vee M = M \times p_- \cup p_+ \times M$. It is well-known that the diagonal map $d_0\colon S\Omega \to S\Omega \times S\Omega$ is homotopic to $i_1 + i_2$, where

$$(i_1 + i_2)[\omega, t] = \begin{cases} [\omega, 2t] \times p_- & \text{if } 0 \leqq t \leqq \frac{1}{2} \\ p_+ \times [\omega, 2t - 1] & \text{if } \frac{1}{2} \leqq t \leqq 1. \end{cases}$$

A homotopy from d_0 to $i_1 + i_2$ is given by

$$\begin{aligned} d_u[\omega, t] &= [\omega, t + ut] \times [\omega, t - ut] \quad \text{if } 0 \leqq t \leqq \tfrac{1}{2} \\ &= [\omega, t + u(1 - t)] \times [\omega, (1 + u)t - u] \ \text{if } \tfrac{1}{2} \leqq t \leqq 1. \end{aligned}$$

Let $\bar{M}$ be the mapping cylinder of $k \times k\colon S\Omega \times S\Omega \to X \times X$, and $\zeta\colon \bar{M} \subset M \times M$ the embedding defined by

$$\zeta([\omega, t], [\omega', t'], u) = (([\omega, t], u), ([\omega', t'], u)).$$

We define a map $d'\colon M \to M \times M$ by

$$d'([\omega, t], u) = \zeta((d_{1-u}[\omega, t]), u). \tag{4.5}$$

Let $d\colon M \to M \times M$ be the diagonal map. It is easily verified that

$$d' \mid S\Omega = i_1 + i_2, \quad d' \mid X = d \mid X, \ \text{and} \ d' \simeq d \operatorname{rel} X;$$

in particular, as a map of pairs, $d'\colon (M, S\Omega) \to (M \times M, M \vee M)$.

Let $(M \vee M)^*$ be the cone on $M \vee M$, let M' be the union $M \times M \cup (M \vee M)^*$ such that $(M \times M) \cap (M \vee M)^* = M \vee M$, and let

$$a\colon (M \times M, M \vee M) \to (M', (M \vee M)^*)$$

be the inclusion. Then d' and a induce maps of the path spaces

$$\begin{tikzcd} E_{S\Omega, M}(M) \arrow[r] \arrow[d, "p"'] & E_{M \vee M, M \times M}(M \times M) \arrow[r] \arrow[d, "p_2"'] & E_{(M \vee M)^*, M'}(M') \arrow[d, "p_3"'] \\ M \arrow[r, "d'"] & M \times M \arrow[r, "a"] & M' \end{tikzcd}$$

which, restricted to the fibres, yield maps (abbreviating $x_0 \times x_0$ by x_0)

$$F = E_{S\Omega, x_0}(M) \xrightarrow{d_1'} E_{M \vee M, x_0}(M \times M) \xrightarrow{a_1} E_{(M \vee M)^*, x_0}(M').$$

Since the transgression and homology suspension are natural, the above maps of fibre spaces, and the corresponding ones for $p^{\#}$, $p_2{}^{\#}$, $p_3{}^{\#}$ (cf. § 2), yield a commutative diagram for $i \geqq 2$.

$$\begin{tikzcd}
H_i(X) \arrow[d, "d_*"'] & H_i(M) \arrow[l, "r_*"'] \arrow[r, "\tau"] \arrow[d, "d'_*"'] & H_{i-1}(E_{S\Omega,x_0}(M)) \arrow[r, "\sigma^{\#}"] \arrow[d, "d'_{1*}"'] & H_i(M, S\Omega) \arrow[d, "d'_*"'] \\
H_i(X \times X) \arrow[d, "a_*"'] & H_i(M \times M) \arrow[l, "(r \times r)_*"'] \arrow[r, "\tau_2"] \arrow[d, "a_*"'] & H_{i-1}(E_{M \vee M, x_0}(M \times M)) \arrow[r, "\sigma_2{}^{\#}"] \arrow[d, "a_{1*}"'] & H_i(M \times M, M \vee M) \arrow[d, "a_*"'] \\
H_i(X') & H_i(M') \arrow[l, "r'_*"'] \arrow[r, "\tau_3"] & H_{i-1}(E_{(M \vee M)^*, x_0}(M')) \arrow[r, "\sigma_3{}^{\#}"] & H_i(M', (M \vee M)^*).
\end{tikzcd}$$

Here $X \vee X = X \times x_0 \cup x_0 \times X$, and we have used the same notation as for M: $(X \vee X)^*$ is the cone on $X \vee X$, $X' = X \times X \cup (X \vee X)^*$ and d and a are the diagonal and inclusion maps. r' is induced by r; since r is a homotopy equivalence, r'_* is an isomorphism for all i. τ, τ_2 and τ_3 are transgressions: τ and τ_2 are defined for $i \leqq 3n+1$, τ_3 for $i \leqq 4n+2$. $\sigma^{\#}$, $\sigma_2{}^{\#}$ and $\sigma_3{}^{\#}$ are the generalized suspensions of § 2; by Proposition (2.4), $\sigma^{\#}$ and $\sigma_2{}^{\#}$ are isomorphisms for $i-1 < 3n+1$, $\sigma_3{}^{\#}$ for $i-1 < 4n+2$. Hence, if we define $\theta'_3\colon H_{i-1}(E_{S\Omega,x_0}(M)) \to H_i(X')$ by $\theta'_3 = r'_*\tau_3{}^{-1}\sigma_3{}^{\#-1}a_*d'_*\sigma^*$ for $i \leqq 4n+2$, then we have a commutative diagram

$$\begin{tikzcd}
H_i(M) \arrow[r, "\tau"] \arrow[d, "r_*"'] & H_{i-1}(E_{S\Omega,x_0}(M)) \arrow[d, "\theta'_3"'] \\
H_i(X) \arrow[r, "a_* d_*"] & H_i(X').
\end{tikzcd} \tag{4.7}$$

(4.8) Lemma. *Let X be n-connected, $n \geqq 2$.* Then $d'_*\colon H_i(M, S\Omega) \to H_i(M \times M, M \vee M)$ *is an isomorphism for $i \leqq 3n$, and an epimorphism for $i = 3n+1$.*

The proof is given in the appendix.

Using the following commutative diagram of injections, we can state (4.7) in a more convenient form:

$$\begin{tikzcd}
H_i(X \times X) \arrow[r, "a_*"] \arrow[d, "b_*"'] & H_i(X') \arrow[d, "b'_*"] \\
H_i(X \times X, X \vee X) \arrow[r, "a'_*"] & H_i(X', (X \vee X)^*).
\end{tikzcd}$$

a'_* is an isomorphism by excision, and b'_* is an isomorphism for $i > 0$; hence we may define $\theta_3\colon H_{i-1}(E_{S\Omega,x_0}(M)) \to H_i(X \times X, X \vee X)$ by $\theta_3 = a'^{-1}_* b'_* \theta'_3$. Abbreviating $b_* d_*$ by d_*, and reverting to the notation $F = E_{S\Omega,x_0}(M)$, we have

(4.9) PROPOSITION. *There exists a commutative diagram for* $1 < i \leqq 4n + 2$

$$\begin{tikzcd}
H_i(M) \arrow[r, "\tau"] \arrow[d, "r_*"'] & H_{i-1}(F) \arrow[d, "\theta_3"'] \\
H_i(X) \arrow[r, "d_*"] & H_i(X \times X, X \vee X)
\end{tikzcd}$$

such that if $n \geqq 2$, *then* θ_3 *is an isomorphism for* $i < 3n + 1$ *and an epimorphism for* $i = 3n + 1$.

Results which are dual to the above hold for cohomology: Firstly, the dual Serre sequence is

$$(4.10)\quad H^{3n+1}(F) \xleftarrow{i^*} H^{3n+1}(E_{S\Omega,M}(M)) \xleftarrow{p^*} H^{3n+1}(M) \xleftarrow{\tau^*} H^{3n}(F) \leftarrow \cdots.$$

Secondly, the following diagram is commutative for $i > 1$:

$$(4.11)\quad \begin{tikzcd}
H^i(F) & H^i(E_{S\Omega,M}(M)) \arrow[l, "i^*"'] & H^i(M) \arrow[l, "p^*"'] \\
H^i(\Omega \times \Omega, \Omega \vee \Omega) \arrow[u, "\theta_1^*"'] & H^{i-1}(\Omega) \arrow[l, "\rho^*"'] \arrow[u, "\theta_2^*"'] & H^i(X), \arrow[l, "\sigma^*"'] \arrow[u, "r^*"']
\end{tikzcd}$$

where all the homomorphisms are the duals of those previously defined; and finally, there is a commutative diagram for $1 < i \leqq 4n + 2$

$$(4.12)\quad \begin{tikzcd}
H^i(M) & H^{i-1}(F) \arrow[l, "\tau^*"'] \\
H^i(X) \arrow[u, "r^*"] & H^i(X \times X, X \vee X) \arrow[l, "d^*"'] \arrow[u, "\theta_3^*"]
\end{tikzcd}$$

such that if $n \geqq 2$, then $\theta_3{}^*$ is an isomorphism for $i < 3n + 1$ and a monomorphism for $i = 3n + 1$.

Hence, with the one exception that $\theta_3{}^*$ has only been proved a monomorphism in dimension $3n + 1$, we have shown that, for $n \geqq 2$, the sequence

$$G(\mu, t, \nu) = ((\mu\nu)_{0,t}\mu_{2t,1}, t, \omega)$$
$$= (\mu_{0,2t}\mu_{2t,1}, t, \omega)$$
$$H(\mu, t, \nu) = (\mu, t, \omega)$$
$$= (\mu, t, \mu_{2t,1}{}^{-1}\{0, \tfrac{1}{2}\}\mu_{2t,1}\{\tfrac{1}{2}, c\}\nu\{c, 1\}),$$

where $c = (3 - 4t)/(4 - 4t)$. For $\frac{1}{2} \leqq t \leqq 1$, setting $\tau = (\mu\nu)_{0,t}\nu_{0,2t-1}{}^{-1}$,

$$G(\mu, t, \nu) = (\tau, t, \nu_{0,2t-1}(\mu\nu)_{t,1})$$
$$= (\tau, t, \nu_{0,2t-1}\nu_{2t-1,1})$$
$$H(\mu, t, \nu) = (\tau, t, \nu)$$
$$= (\mu\{0, e\}\nu_{0,2t-1}\{e, \tfrac{1}{2}\}\nu_{0,2t-1}{}^{-1}\{\tfrac{1}{2}, 1\}, t, \nu),$$

where $e = 1/(4t)$.

II) The composition $hh'\colon F \rightarrow F$ is given by

$$hh'(\alpha) = \lambda[(\omega_{0,t}\beta)(\beta^{-1}\omega_{t,1}), t](\omega_{0,t}\beta)_{2t,1} \qquad \text{if } 0 \leqq t \leqq \tfrac{1}{2}$$
$$\lambda[(\omega_{0,t}\beta)(\beta^{-1}\omega_{t,1}), t](\beta^{-1}\omega_{t,1})_{0,2t-1}{}^{-1} \qquad \text{if } \tfrac{1}{2} \leqq t \leqq 1.$$

Let $T\colon F \rightarrow F$ be given by $T(\alpha) = \lambda[\omega, t]\beta$; then $T \cong 1'$, where $1'$ is the identity map of F. Using the above deformations of paths, we shall indicate a homotopy $hh' \cong T$ for $0 \leqq t \leqq \frac{1}{4}$; closely analogous homotopies can be given for the other three quarters of the unit t-interval. $hh' \cong H_1 \cong H' \cong T$, where H_1 and H' are defined for $0 \leqq t \leqq \frac{1}{4}$ as follows: Let H_s be the homotopy given by

$$H_s(\alpha) = \lambda[\omega_{0,t}\{0, a\}\beta\{a, \tfrac{1}{2}\}\beta^{-1}\{\tfrac{1}{2}, \tfrac{3}{4}\}\omega_{t,1}\{\tfrac{3}{4}, 1\}, t]\{0, \tfrac{1}{2}\}\omega_{b,t}\{\tfrac{1}{2}, d\}\beta\{d, 1\},$$

where $a = (4ts - s + 1)/4$, $b = 4t^2/(4ts - s + 1)$, and $d = (3 - 8t)/(4 - 8t)$. Then $H_0(\alpha) = hh'(\alpha)$, and

$$H_1(\alpha) = \lambda[\omega_{0,t}\{0, t\}\beta\{t, \tfrac{1}{2}\}\beta^{-1}\{\tfrac{1}{2}, \tfrac{3}{4}\}\omega_{t,1}\{\tfrac{3}{4}, 1\}, t]\{0, \tfrac{1}{2}\}\omega_{t,t}\{\tfrac{1}{2}, d\}\beta\{d, 1\}$$
$$H'(\alpha) = \lambda[\omega_{0,t}\{0, t\}\omega_{t,1}\{t, 1\}, t]\{0, \tfrac{1}{2}\}\omega_{t,t}\{\tfrac{1}{2}, d\}\beta\{d, 1\}$$
$$= \lambda[\omega, t]\{0, \tfrac{1}{2}\}\omega_{t,t}\{\tfrac{1}{2}, d\}\beta\{d, 1\}$$
$$T(\alpha) = \lambda[\omega, t]\{0, \tfrac{1}{2}\}\beta\{\tfrac{1}{2}, 1\}.$$

(A. 2) *Proof of Lemma* (4. 8).

We shall first prove that if X is n-connected, $n \geqq 2$, then $d'_*\colon \pi_i(M, S\Omega) \rightarrow \pi_i(M \times M, M \vee M)$ is an isomorphism for $i < 3n + 1$ and an epimorphism for $i = 3n + 1$. Consider the following diagram (since all spaces are 1-connected, we may neglect base-points):

(A. 3)

$$\begin{tikzcd}
0 \arrow[r] & \pi_{i+1}(M, S\Omega) \arrow[rrr, "\partial"] \arrow[dd, "d'_*"'] \arrow[dr, phantom, "1"] & & & \pi_i(S\Omega) \arrow[rrr, "j_*"] \arrow[dl, "H"'] \arrow[d, "u_*"] \arrow[dr, "d_*"] \arrow[drr, phantom, "2"] & & & \pi_i(M) \arrow[r] \arrow[dd, "d_*"] & 0 \\
& & 0 \arrow[r] & \pi_{i+1}(S\Omega \times S\Omega, S\Omega \vee S\Omega) \arrow[r, "\partial'"] \arrow[dll, "(j \times j)_*"'] \arrow[d, phantom, "3"] & \pi_i(S\Omega \vee S\Omega) \arrow[r, shift left, "j'_*"] \arrow[d, "(j \vee j)_*"] \arrow[dr, phantom, "4"] & \pi_i(S\Omega \times S\Omega) \arrow[l, shift left, "f"] \arrow[r] \arrow[drr, "(j \times j)_*"] & 0 & & \\
0 \arrow[r] & \pi_{i+1}(M \times M, M \vee M) \arrow[rrr, "\partial''"] & & & \pi_i(M \vee M) \arrow[rrr, shift left, "j''_*"] & & & \pi_i(M \times M) \arrow[lll, shift left, "g"] \arrow[r] & 0
\end{tikzcd}$$

Here $u: S\Omega \to S\Omega \vee S\Omega$ shrinks the equator $\Omega \subset S\Omega$ to a point, so that $j'u = i_1 + i_2$, where $j': S\Omega \vee S\Omega \to S\Omega \times S\Omega$ is the inclusion. It is well-known that the lower two sequences split; f and g are the canonical right inverses for j'_* and j''_* respectively. Finally, H is defined by the equation $u_* = \partial' H + f d_*$. The diagram does not commute, but we indicate such commutativity relations as exist.

Note first that $(j \vee j) u = d' \mid S\Omega : S\Omega \to M \vee M$. Hence the two large squares commute: $(j \vee j)_* u_* \partial = \partial'' d'_*$ and $j''_* (j \vee j)_* u_* = d_* j_*$. Squares 2, 3 and 4 clearly are commutative; we shall show that 1 is also.

$(j \vee j)_* u_* \partial = (j \vee j)_* f d_* \partial + (j \vee j)_* \partial' H \partial$; however,

$(j \vee j)_* f d_* \partial = g (j \times j)_* d_* \partial = g d_* j_* \partial = 0$. Hence

$(j \vee j)_* u_* \partial = (j \vee j)_* \partial' H \partial = \partial'' (j \times j)_* H \partial$.

But $(j \vee j)_* u_* \partial = \partial'' d'_*$; hence $\partial'' d'_* = \partial'' (j \times j)_* H \partial$, from which it follows that $d'_* = (j \times j)_* H \partial$, since ∂'' is a monomorphism. Therefore square 1 is commutative.

We shall next show that $H\partial$ and $(j \times j)_*$ are isomorphisms under suitable conditions; this will imply that d'_* is also an isomorphism. Consider the following diagram:

(A. 4)

$$\begin{tikzcd}
 & & & \pi_{i+1}(M, S\Omega) \arrow[dl, "\partial"'] \arrow[d, "\gamma", "3"'] & 0 \arrow[l] \\
0 \arrow[r] & \pi_{i-1}(\Omega) \arrow[r, "E"] & \pi_i(S\Omega) \arrow[r, "i_*"] \arrow[dl, "k_*"] \arrow[ddl, "j_*"] \arrow[ddr, "u_*"] \arrow[dddr, "H"'] & \pi_i(S\Omega; \Omega_+, \Omega_-) \arrow[r] \arrow[d, "u'_*", "4"'] & 0 \\
0 & \pi_i(X) \arrow[l] \arrow[u, "-\sigma^{-1}", "1"'] & & \pi_i(S\Omega \vee S\Omega; S\Omega, S\Omega) & \\
0 & \pi_i(M) \arrow[l] \arrow[u, "r_*", "2"'] & & \pi_i(S\Omega \vee S\Omega) \arrow[u, "n_*"'] & \\
 & & & \pi_{i+1}(S\Omega \times S\Omega, S\Omega \vee S\Omega) \arrow[u, "\partial'"'] &
\end{tikzcd}$$

The horizontal exact sequence is part of the triad suspension sequence [7]; since by (2.7) E is a monomorphism, i_* is an epimorphism. n_* is the injection, and γ is defined to be $i_*\partial$. The numbered triangles and squares are commutative.

(A. 5) LEMMA. *γ is an isomorphism.*

Proof. 1) kernel $\gamma =$ kernel $i_* \cap$ image $\partial =$ image $E \cap$ kernel k_* by exactness. But image $E \cap$ kernel $k_* = 0$, since $-\sigma^{-1}k_*E =$ identity. Hence kernel $\gamma = 0$.

2) Let $a \in \pi_i(S\Omega; \Omega_+, \Omega_-)$. Since i_* is an epimorphism, there exists $a' \in \pi_i(S\Omega)$ such that $i_*(a') = a$. Let $a'' = a' + E\sigma^{-1}k_*(a')$. Then

$$i_*(a'') = i_*(a') + i_*E\sigma^{-1}k_*(a') = a. \quad \text{Also,}$$

$$k_*(a'') = k_*(a') + k_*E\sigma^{-1}k_*(a') = k_*(a') - k_*(a') = 0;$$

hence there exists $b \in \pi_{i+1}(M, S\Omega)$ such that $\partial(b) = a''$, and therefore $\gamma(b) = i_*\partial(b) = i_*(a'') = a$. Therefore γ is an epimorphism.

(A. 6) LEMMA. *$H\partial\colon \pi_{i+1}(M, S\Omega) \to \pi_{i+1}(S\Omega \times S\Omega, S\Omega \vee S\Omega)$ is an isomorphism for $2 < i + 1 \leqq 3n$ and an epimorphism for $i + 1 = 3n + 1$.*

Proof. Blakers and Masey have shown ([2], Corollary 8.3) that $n_*\partial'$ is an isomorphism for $i + 1 > 2$; hence it suffices to consider $n_*\partial' H\partial$. Note that $n_*f = 0$. Hence

$$n_*\partial' H\partial = n_*u_*\partial - n_*fd_*\partial = n_*u_*\partial = u'_*i_*\partial = u'_*\gamma. \tag{A. 7}$$

Let Ω^* be the cone on Ω, $S\Omega^* = S\Omega \cup \Omega^*$ such that $S\Omega \cap \Omega^* = \Omega$, and let Ω_+^*, Ω_-^* be the subspaces $\Omega_+ \cup \Omega^*$, $\Omega_- \cup \Omega^*$ of $S\Omega^*$. It follows from Corollary (3.5) of [10] that the injection

$$u''_*\colon \pi_i(S\Omega\,;\Omega_+,\Omega_-) \to \pi_i(S\Omega^*\,;\Omega_+^*,\Omega_-^*)$$

is an isomorphism for $i < 3n$, and an epimorphism for $i = 3n$.

We denote points of $u(\Omega_-) \subset S\Omega \vee S\Omega$ by $u[\omega, t] = [\omega, 2t]$, $0 \leqq t \leqq \frac{1}{2}$, and those of $u(\Omega_+)$ by $u[\omega, t] = [\omega, 2t - 1]'$, $\frac{1}{2} \leqq t \leqq 1$. Points of $\Omega^* \subset S\Omega^*$ will be denoted $[\omega, s]$, $\frac{1}{2} \leqq s \leqq 1$, with $[\omega, 1] = [\omega', 1]$ for all $\omega, \omega' \in \Omega$. Define maps

$$S\Omega^* \xrightarrow{\alpha} S\Omega \vee S\Omega \xrightarrow{\beta} S\Omega^*$$

by $\alpha \mid S\Omega = u$, $\alpha(\Omega^*) = u(\Omega)$,

$$\begin{aligned} \beta[\omega, t] &= [\omega, t] \in \Omega_- && \text{for } 0 \leqq t \leqq \tfrac{1}{2} \\ &= [\omega, t] \in \Omega^* && \text{for } \tfrac{1}{2} \leqq t \leqq 1; \\ \beta[\omega, t]' &= [\omega, 1 - t] \in \Omega^* && \text{for } 0 \leqq t \leqq \tfrac{1}{2} \\ &= [\omega, t] \in \Omega_+ && \text{for } \tfrac{1}{2} \leqq t \leqq 1. \end{aligned}$$

Then it is easy to see that $\alpha\beta \simeq$ identity, $\beta\alpha \simeq$ identity, and that α is a homotopy equivalence of triads $\alpha\colon (S\Omega^*\,;\Omega_+^*,\Omega_-^*) \to (S\Omega \vee S\Omega\,; S\Omega, S\Omega)$. Hence $\alpha_*\colon \pi_i(S\Omega^*\,;\Omega_+^*,\Omega_-^*) \to \pi_i(S\Omega \vee S\Omega\,; S\Omega, S\Omega)$ is an isomorphism for all i. Since $\alpha u'' = u'$, it follows that u'_* is an isomorphism for $i < 3n$ and an epimorphism for $i = 3n$. Since γ is an isomorphism, (A.7) implies that $n_*\partial' H\partial$, and hence $H\partial$, is an isomorphism for $i + 1 \leqq 3n$, and an epimorphism for $i + 1 = 3n + 1$. This completes the proof of (A.6).

(A.8) LEMMA. *$(j \times j)_*\colon \pi_i(S\Omega \times S\Omega, S\Omega \vee S\Omega) \to \pi_i(M \times M, M \vee M)$ is an isomorphism for $i \leqq 3n + 1$.*

Proof. We shall first prove that $(j \times j)_*$ is an isomorphism in homology, and then use a standard method to transfer the result to homotopy. Consider

$$\text{(A.9)}\qquad \begin{tikzcd} H_i(M \times M, M \vee M) \arrow[r, "a_*"] & H_i(M', (M \vee M)^*) & H_i(M') \arrow[l, "b_*"'] \\ H_i(S\Omega \times S\Omega, S\Omega \vee S\Omega) \arrow[u, "(j \times j)_*"] \arrow[r, "a_*"] & H_i(S\Omega', (S\Omega \vee S\Omega)^*) \arrow[u] & H_i(S\Omega') \arrow[l, "b_*"'] \arrow[u, "(j \times j)'_*"'] \end{tikzcd}$$

where $S\Omega' = S\Omega \times S\Omega \cup (S\Omega \vee S\Omega)^*$, and similarly for M', and where a_* and b_* are injections. a_* is an isomorphism for all i by excision, b_* for $i > 0$ by exactness. Since there are contractible neighborhoods of the points p_+ and p_- in $S\Omega$ and in M, we may apply the relative Künneth formula: since $j_*\colon H_i(S\Omega, p_\pm) \to H_i(M, p_\pm)$ is an isomorphism for $i \leqq 2n$ and an epimorphism for $i = 2n+1$, the formula implies that $(j \times j)_*$ is an isomorphism for $i \leqq 3n+1$ and an epimorphism for $i = 3n+2$. By commutativity of (A. 9), the same result therefore holds for $(j \times j)'_*$. Hence by exactness, $H_i(M', S\Omega') = 0$ for $i \leqq 3n+2$. Using the relative Hurewicz theorem, $\pi_i(M', S\Omega') = 0$ for $i \leqq 3n+2$, and by exactness $(j \times j)'_*\colon \pi_i(S\Omega') \to \pi_i(M')$ is an isomorphism for $i \leqq 3n+1$. Now if we rewrite diagram (A. 9) for homotopy, then the corresponding injection b_* is an isomorphism for all i, while by Corollary (3. 3) of [10], a_* is an isomorphism for $i \leqq 3n+1$. Hence $(j \times j)_*$ is an isomorphism for $i \leqq 3n+1$, which proves (A. 8).

It follows from (A. 6), (A. 8), and the commutativity relations in (A. 3) that $d'_*\colon \pi_i(M, S\Omega) \to \pi_i(M \times M, M \vee M)$ is an isomorphism for $i < 3n+1$ and an epimorphism for $i = 3n+1$. By reversing the standard argument used in the proof of (A. 8) to transform the homology isomorphism into a homotopy isomorphism, we conclude that (4. 8) holds.

Part II. Eilenberg-MacLane Spaces.

1. **Introduction.** In order to replace CW-complexes by Postnikov systems, one must know the effect which standard operations on complexes have on the corresponding Postnikov invariants. This is known for the loop space [16], but seems more complicated for suspension. The following proposition determines the invariants of the suspension within the stable range:

Let X be an n-connected CW-complex, $n \geqq 1$, let $q \leqq 2n-1$, and let X_q, $(SX)_{q+1}$ be the q-th and $(q+1)$-st spaces in Postnikov systems for X and SX respectively (cf. § 3 below); then there exists a $(2n+2)$-equivalence $h\colon S(X_q) \to (SX)_{q+1}$. We identify $\pi = \pi_{q+1}(X)$ with $\pi_{q+2}(SX)$ and $\pi_{q+1}(\Omega SX)$ under E and σE.

(1.1) Proposition. *If $k^{q+3} \in H^{q+3}((SX)_{q+1}; \pi)$ is a Postnikov invariant for SX, then $-E^*h^*k^{q+3}$ is an invariant for X.*

Proof. The following diagram of isomorphisms is commutative, where h' is induced by h, $i\colon X_q \to \Omega S(X_q)$ is the standard embedding and all coefficients are π:

$$\begin{tikzcd}
H^{q+2}(X_q) & H^{q+3}(S(X_q)) \arrow[l, "-E^*"'] \arrow[d, "\sigma^*"] & H^{q+3}((SX)_{q+1}) \arrow[l, "h^*"'] \arrow[d, "\sigma^*"] \\
 & H^{q+2}(\Omega S(X_q)) \arrow[ul, "i^*"] & H^{q+2}(\Omega((SX)_{q+1})) \arrow[l, "h'^*"']
\end{tikzcd}$$

$\sigma^* k^{q+3}$ is an invariant for ΩSX [16]; since $h'i\colon X_q \to \Omega((SX)_{q+1})$ is a homotopy equivalence, $i^* h'^* \sigma^* k^{q+3} = -E^* h^* k^{q+3}$ is also an invariant for ΩSX. Since the embedding $i\colon X \to \Omega SX$ is a $2n$-equivalence, a Postnikov system up to dimension $2n$ (i.e., up to X_{2n-1}, k^{2n+1}) for ΩSX is also a system for X. This proves the proposition.

The simplest category in which to investigate the non-stable case would seem to be that of Eilenberg-MacLane spaces. Our aim is to apply the results of Part I to the computation of some of the invariants of such spaces.

According to [9], the category of spaces having the homotopy type of CW-complexes is closed under the operations of Part I; we shall assume that all spaces which we consider are in this category. Let $K(\pi, n+1)$ be a CW-complex which is an Eilenberg-MacLane space of type $(\pi, n+1)$ (briefly, a $(\pi, n+1)$-space) and let $K = \Omega K(\pi, n+1)$; then K is a (π, n)-space.

2. Homotopy groups of *SK*. The fundamental map $k\colon SK \to K(\pi, n+1)$ is equivalent to a fibre map in which the fibre has the homotopy type of $K * K$; hence there is an exact sequence, which splits (I, (2.7)):

$$(2.1) \qquad 0 \to \pi_i(K * K) \to \pi_i(SK) \xrightarrow{k_*} \pi_i(K(\pi, n+1)) \to 0.$$

Consequently we have

(2.2) PROPOSITION.

$$\pi_i(SK) = 0,\ i \leqq n;\ \pi_{n+1}(SK) \approx \pi;\ \pi_i(SK) \approx \pi_i(K * K),\ i \geqq n+2.$$

(2.3) COROLLARY.

$$\pi_i(SK) = 0,\ n+1 < i < 2n+1;\ \pi_{2n+s+1}(SK) \approx H_{n+s}(\pi, n; \pi), \quad 0 \leqq s \leqq n-1.$$

Proof. Since K is $(n-1)$-connected, $K * K$ is $2n$-connected, and the first statement follows. The second statement follows from (2.2) and Theorem 6.1 of [19].

In particular, $\pi_{2n+1}(SK) \approx \pi \otimes \pi$, $\pi_{2n+2}(SK) \approx \pi * \pi$.

3. Moore-Postnikov systems [11].

In this section, let $f\colon E \to B$ be a fibre map in which B and the fibre F are 1-connected.

(3.1) *Definition.* A sequence of spaces and maps (E_n, g_n, h_n) is a *Moore-Postnikov system* [11] for the fibre map f if:

(1) $g_n\colon E_n \to E_{n-1}$ is a fibre map with fibre a $(\pi_n(F), n)$-space.

(2) $h_n\colon E \to E_n$ is an n-equivalence.

(3) $E_0 = B$, $h_0 = f$, and $h_n = g_{n+1}h_{n+1}$.

We denote the composition $g_1 g_2 \cdots g_n\colon E_n \to B$ by f_n, and set $F_n = f_n^{-1}(b)$, where $b \in B$.

(3.2) *Definition.* A *Postnikov system* [13] for a space E is a Moore-Postnikov system for the trivial fibre map $f\colon E \to B$, where B is a single point.

(3.3) THEOREM. *Any fibre map has a Moore-Postnikov system.*

The theorem is a consequence of the existence of semi-simplicial Moore-Postnikov systems ([11], Theorem 2.12) and of results of Barratt, Gugenheim and Moore on the geometric realization of certain classes of semi-simplicial fibre spaces (to appear).

Using (3.3), one readily verifies that if F is m-connected, then a Moore-Postnikov system (E_n, g_n, h_n) may be constructed such that $E_i = B$, $h_i = f$, $g_i =$ identity, $i \leqq m$.

(3.4) *Definition.* Let (E_n, g_n, h_n) be a Postnikov system for a space E, $\mathcal{F}_{n+1}$ the fibre of $g_{n+1}\colon E_{n+1} \to E_n$, and $b^{n+1} \in H^{n+1}(\mathcal{F}_{n+1}, \pi_{n+1}(\mathcal{F}_{n+1}))$ the basic class. Then if τ is the transgression in the fibering g_{n+1},

$$-\tau b^{n+1} \in H^{n+2}(E_n, \pi_{n+1}(\mathcal{F}_{n+1}))$$

is denoted by $k^{n+2}(E)$ and is called an $(n+2)$nd *Postnikov invariant* of E.

Let Φ be the group of automorphisms of $H^{n+2}(E_n, \pi_{n+1}(\mathcal{F}_{n+1}))$ determined by homotopy equivalences of E_n and automorphisms of $\pi_{n+1}(\mathcal{F}_{n+1})$, and let $\{k^{n+2}\}$ be the equivalence class of k^{n+2} under Φ. We identify $\pi_{n+1}(F_{n+1}) \approx \pi_{n+1}(E_{n+1})$ under injection.

(3.5) PROPOSITION. *Let (E_n, g_n, h_n), (E'_n, g'_n, h'_n) be two Postnikov systems for a space E. Then*

(1) *They are equivalent in the sense that there exists a sequence of homotopy equivalences $\lambda_n\colon E_n \to E'_n$.*

(2) $\lambda_{n+1*}{}^{-1}\lambda_{\pi}{}^{*}k'^{n+2} \in \{k^{n+2}\}$, *where* $\lambda_{n+1*} : \pi_{n+1}(\mathcal{F}_{n+1}) \to \pi_{n+1}(\mathcal{F}'_{n+1})$ *is the coefficient isomorphism.*

(3) *Given* $l \in \{k^{n+2}\}$, *there exists a Postnikov system* (E''_i, g''_i, h''_i) *for* E *in which* $E''_i = E_i$, $g''_i = g_i$, and $h''_i = h_i$, $i \leqq n$, *and such that* $l = -\tau b^{n+1}$.

This proposition is an analogue for fibre spaces of a theorem of Adams[1] on self-obstructions; we omit the proof. It follows that the invariant object is actually the class $\{k^{n+2}\}$, although we shall continue to speak of the elements k^{n+2}. It also follows that we may calculate Postnikov invariants modulo coefficient isomorphisms.

4. **A Postnikov system for $SK(\pi, n)$.** Consider the fibre map $p : E \to M$, with fibre F, described in Part I, § 3, where $E = E_{S\Omega,M}(M)$, M is the mapping cylinder of $k : S\Omega \to X$ and $X = K(\pi, n+1)$ is a CW-complex. Let (E_i, g_i, h_i) be a Moore-Postnikov system for E in which $E_i = M$, $g_i =$ identity, and $h_i = p$, $i \leqq n+1$. Note that a Postnikov system (E'_i, g'_i, h'_i) for E is obtained by setting

$$E'_i = E_i,\ g'_{i+1} = g_{i+1},\ h'_i = h_i \text{ for } i \geqq n+1;$$

$$E'_i = *,\ g'_{i+1} = *,\ h'_i = *, \quad i < n+1,$$

where $*$ denotes a space consisting of a single point or the map into $*$. Since $E \equiv SK(\pi, n)$,[3] this is also a Postnikov system for the latter space.

(4.1) THEOREM.[4] $k^{i+1}(F) = 0$ *for* $i \leqq 3n$, *so that* $F_{3n} \equiv \prod_{j=1}^{3n} K(\pi_j(F), j)$.

(4.2) LEMMA. [8] *If* Y *is a* 1*-connected space, then* $k^{i+1}(Y) = 0$ *if and only if the Hurewicz homomorphism* $\mathcal{H} : \pi_i(Y) \to H_i(Y)$ *is a monomorphism onto a direct summand.*

(4.3) LEMMA. $\mathcal{H} : \pi_i(K * K) \to H_i(K * K)$ *is a monomorphism onto a direct summand for* $i \leqq 3n$, *where* K *is a* (π, n)*-space.*

The proof of (4.3) will be given later. Since $F \equiv K * K$, (4.1) follows from (4.2) and (4.3).

For the statement and proof of (4.4), i is to be a fixed positive integer, $i \leqq 3n$. Consider the following commutative diagram, in which the notation is that of § 3:

---

[3] We write $X \equiv Y$ to indicate that X and Y have the same homotopy type.

[4] This is a generalization of our earlier results, which was noted after the submission of the original version of the paper; it was also remarked by the referee, whom the authors wish to thank for several useful suggestions.

$$\begin{tikzcd}
E \arrow[r, "h_i"] \arrow[d, "p"'] & E_i \arrow[d, "p_i"] & E_i \arrow[l, "="'] \arrow[d, "g_i"] \\
M \arrow[r, "="'] & M & E_{i-1} \arrow[l, "p_{i-1}"]
\end{tikzcd}$$

h_i induces by restriction to the respective fibres a map $h'_i\colon F \to F_i$ which is an i-equivalence, while p_{i-1} induces similarly a map $p_{i-1}'\colon \mathfrak{F}_i \to F_i$ such that $p_{i-1}'{}_*\colon \pi_i(\mathfrak{F}_i) \to (F_i)$ is an isomorphism. Since $\mathfrak{H}$ is natural, $p_{i-1}'{}_* H_i(\mathfrak{F}_i) = \mathfrak{H}\pi_i(F_i)$.

Choose a left inverse $\mathfrak{H}_F^-$ for the Hurewicz homomorphism $\mathfrak{H}_F\colon \pi_i(F) \to H_i(F)$ and let $a^i(F) \in H^i(F, \pi_i(F))$ be an element such that $\alpha(a^i(F)) = \mathfrak{H}_F^-$, where $\alpha\colon H^i(F,\pi_i(F)) \to \operatorname{Hom}(H_i(F), \pi_i(F))$ is the homomorphism of the universal coefficient theorem. We shall initially compute $k^{i+1}(E)$ in terms of this class.

(4.4) Proposition. *For $i \leqq 3n$, Postnikov invariants for E are given by $k^{i+1}(E) = -p_{i-1}{}^*\tau a^i(F) \in H^{i+1}(E_{i-1}, \pi_i(F))$, where τ is the transgression in the fibre space (E, M, p).*

Proof. Let τ_1, τ_2 be the transgressions in the fiberings $E_i \to M$ and $E_i \to E_{i-1}$ respectively. We identify $\pi_i = \pi_i(F) = \pi_i(F_i) = \pi_i(\mathfrak{F}_i)$ under h'_{i*} and p'_{i-1*}. Consider the following diagram, in which we abbreviate $h' = h'_i$ and $p' = p'_{i-1}$:

$$\begin{tikzcd}
\operatorname{Hom}(H_i(\mathfrak{F}_i), \pi_i) & H^i(\mathfrak{F}_i, \pi_i) \arrow[l, "\alpha"', "\approx"] \arrow[r, "\tau_2"] & H^{i+1}(E_{i-1}, \pi_i) \\
\operatorname{Hom}(H_i(F_i), \pi_i) \arrow[u, "{\operatorname{Hom}(p'_*, 1)}"] \arrow[d, "{\operatorname{Hom}(h'_*, 1)}"', "\approx"] & H^i(F_i, \pi_i) \arrow[l, "\alpha"'] \arrow[r, "\tau_1"] \arrow[u, "p'^*"'] \arrow[d, "h'^*"', "\approx"] & H^{i+1}(M, \pi_i) \arrow[u, "p_{i-1}{}^*"'] \arrow[d, "="] \\
\operatorname{Hom}(H_i(F), \pi_i) & H^i(F, \pi_i) \arrow[l, "\alpha"'] \arrow[r, "\tau"] & H^{i+1}(M, \pi_i).
\end{tikzcd}$$

Under the identifications, $\operatorname{Hom}(p'_*, 1)\operatorname{Hom}(h'_*; 1)^{-1}\mathfrak{H}_F^- = \mathfrak{H}^{-1}$. Hence $p'^*h'^{*-1}a^i(F) = b^i(\mathfrak{F}_i)$, and

$$-p_{i-1}{}^*\tau a^i(F) = -\tau_2 p'^* h'^{*-1} a^i(F) = -\tau_2 b^i(\mathfrak{F}_i) = k^{i+1}(E).$$

This proves (4.4). For the remainded of § 4, let $i < 3n$.

Choose a fixed left inverse $\mathfrak{H}^-$ for

$$\mathfrak{H}\colon \pi_i(X \times X, X \vee X) \to H_i(X \times X, X \vee X);$$

that such exists follows readily from (4.3) and the fact that $X*X \equiv S(X \times X/X \vee X)$. By (4.12) of Part I, $\tau a^i(F) = r^*d^*\theta_3^{*-1}a^i(F)$. Now θ_3 is a composition of isomorphisms, each of which has an analogue in homotopy which commutes with $\mathfrak{H}$. Thus we have a commutative diagram

$$\begin{tikzcd}
H_{i+1}(X \times X, X \vee X) \arrow[r, "\theta_3^{-1}"] & H_i(F) \\
\pi_{i+1}(X \times X, X \vee X) \arrow[r, "\theta_3^{-1}"] \arrow[u, "\mathfrak{H}"] & \pi_i(F) \arrow[u, "\mathfrak{H}_F"']
\end{tikzcd}$$

in which θ_3^{-1} is an isomorphism in both cases, and $\mathfrak{H}$ and $\mathfrak{H}_F$ are monomorphisms onto direct summands. Hence if we define a left inverse $\mathfrak{H}_F^-$ by requiring that it commute with $\mathfrak{H}^-$ and identifying under $\theta_3 \colon \pi_i(F) \approx \pi_{i+1}(X \times X, X \vee X)$, then the dual isomorphism $\theta_3^{*-1} \colon H^i(F;\pi_i(F)) \to H^{i+1}(X \times X, X \vee X; \pi_{i+1}(X \times X, X \vee X))$ carries the coset $\alpha^{-1}(\mathfrak{H}_F^-)$ onto the coset $\alpha^{-1}(\mathfrak{H}^-)$; i.e., for each $a^{i+1} = a^{i+1}(X \times X, X \vee X)$ there exists $a^i(F) \in \alpha^{-1}(\mathfrak{H}_F^-)$ such that $\theta_3^{*-1}a^i(F) = a^{i+1}$. Then from (4.4),

$$k^{i+1}(E) = -p_{i-1}^*\tau a^i(F) = -p_{i-1}^*r^*d^*a^{i+1}.$$

We define a new sequence of fiberings by setting

$$E''_0 = X,\quad E''_i = p_i^{-1}(X) \subset E_i,\quad p''_i = p_i \mid E''_i \colon E''_i \to X.$$

Since the inclusion $i_{i-1} \colon E''_{i-1} \subset E_{i-1}$ is a homotopy equivalence, we may replace $k^{i+1}(E)$ by $i_{i-1}^*k^{i+1}(E)$, and the new Postnikov invariant is given by

$$k^{i+1}(E) = -i_{i-1}^*p_{i-1}^*r^*d^*a^{i+1} = -p''_{i-1}{}^*d^*a^{i+1},$$

since $i_{i-1}^*p_{i-1}^* = p''_{i-1}{}^*i^*$ and $i^*r^* =$ identity. Hence

(4.5) PROPOSITION. *Postnikov invariants $k^{i+1}(E)$, $i < 3n$, are given by $k^{i+1}(E) = -p''_{i-1}{}^*d^*a^{i+1}(X \times X, X \vee X)$, where a^{i+1} is any element such that $\alpha(a^{i+1})$ is a left inverse for $\mathfrak{H}$.*[5]

The element $a^{2n+2}(X \times X, X \vee X)$, which is the basic class, is easy to calculate. Since the following diagram of isomorphisms is commutative ([2], 5.11), where μ and ν are the homology and homotopy cross-products,

---

[5] The restriction $i < 3n$ is caused by the dimensional restriction in (4.9) of Part I. If π is finitely-generated, then θ_3 is an epimorphism of the finite group $H_{3n}(F)$ onto an isomorphic group, and therefore an isomorphism. Hence, in this case (4.5) holds for $i \leqq 3n$.

$$\begin{tikzcd}
H_{n+1}(X) \otimes H_{n+1}(X) \arrow[r, "\mu"] & H_{2n+2}(X \times X, X \vee X) \\
\pi_{n+1}(X) \otimes \pi_{n+1}(X) \arrow[u, "\mathfrak{H} \otimes \mathfrak{H}"] \arrow[r, "\nu"] & \pi_{2n+2}(X \times X, X \vee X) \arrow[u, "\mathfrak{H}"']
\end{tikzcd}$$

it follows readily that $a^{2n+2}(X \times X, X \vee X) = b \times b$, with coefficient pairing ν, where $b = b^{n+1}(X)$ is the basic class. Identifying under ν, from (4.5) we obtain

(4.6) COROLLARY.

$$k^{2n+2}(SK(\pi, n)) = -d^*(b \times b) = -b \cup b \in H^{2n+2}(X; \pi \otimes \pi),$$

with the natural coefficient pairing.

We shall next obtain some information concerning the reduced join ([7], § 14) $X \mathbf{X} X = X \times X / X \vee X$ which is needed for (4.10), and in the process shall prove (4.3). Consider the spectral sequence for the homotopy of the join $X * X$, the analogous (trivial) spectral sequence for the homology of $X * X$, and the map of the first into the second induced by the Hurewicz homomorphism ([19], § 5). We are interested in the terms

$$E^1_{s-1,0}(\pi) = \pi_{2n+s+2}(X * X^{n+s}, X * X^{n+s-1}) \xrightarrow{\mathfrak{H}} H_{2n+s+2}(X * X^{n+s}, X * X^{n+s-1})$$
$$= E^1_{s-1,0}(H).$$

It follows easily from Lemmas 5.2, 5.3 of [19] and their analogues for homology that the following diagram commutes for all s,

$$\begin{tikzcd}
E^1_{s,0}(\pi) \arrow[r, "d^1"] \arrow[d, "\mathfrak{H}"'] & E^1_{s-1,0}(\pi) \arrow[d, "\mathfrak{H}"] \\
E^1_{s,0}(H) \arrow[r, "d^1"] & E^1_{s-1,0}(H)
\end{tikzcd}$$

and that the vertical homomorphisms $\mathfrak{H}$ are isomorphisms. Hence $\mathfrak{H}$ induces isomorphisms $\mathfrak{H}_\#: E^2_{s,0}(\pi) \to E^2_{s,0}(H)$. On the other hand, $E^2_{s,0}(H) = E^\infty_{s,0}(H)$ as is well-known, and $E^2_{s,0}(\pi) = E^\infty_{s,0}(\pi)$ for $s \leqq n+1$, by [19], 6.1. Also,

$$E^\infty_{s-1,0}(\pi) \approx \pi_{2n+s+2}(X * X) / i' \pi_{2n+s+2}(X * X^{n+s-1})$$

and similarly for homology. By naturality of the Hurewicz homomorphism, we obtain the following commutative diagram for $s \leqq n+1$, where $\mathfrak{H}_\#$ is an isomorphism:

(4.7)
$$\begin{tikzcd}
H_{2n+s+2}(X*X) \arrow[r, "\eta'"] & H_{2n+s+2}(X*X)/i'H_{2n+s+2}(X*X^{n+s-1}) \\
\pi_{2n+s+2}(X*X) \arrow[r, "\eta''"] \arrow[u, "\mathfrak{H}"] & \pi_{2n+s+2}(X*X)/i'\pi_{2n+s+2}(X*X^{n+s-1}). \arrow[u, "\mathfrak{H}_\#"']
\end{tikzcd}$$

Here η', η'' are the canonical maps, and η'' is an isomorphism for $s \leqq n+1$.

There is a singular homotopy equivalence $\phi\colon Y*Z \to S(Y \mathbf{X} Z)$ by [19], § 7; applying this to (4.7) and de-suspending (this is justified, since $s \leqq n+1$), we obtain the commutative diagram, where $\mathfrak{H}_\#$ and η'' are isomorphisms:

(4.8)
$$\begin{tikzcd}
H_{2n+s+1}(X \mathbf{X} X) \arrow[r, "\eta'"] & H_{2n+s+1}(X \mathbf{X} X)/i'H_{2n+s+1}(X \mathbf{X} X^{n+s-1}) \\
\pi_{2n+s+1}(X \mathbf{X} X) \arrow[r, "\eta''"] \arrow[u, "\mathfrak{H}"] & \pi_{2n+s+1}(X \mathbf{X} X)/i'\pi_{2n+s+1}(X \mathbf{X} X^{n+s-1}). \arrow[u, "\mathfrak{H}_\#"']
\end{tikzcd}$$

One verifies by use of the Künneth formula that η' is the projection onto the direct summand $H_{n+1}(X) \otimes H_{n+s}(X) + H_{n+1}(X) * H_{n+s-1}(X)$.

(4.9) LEMMA. *Let $f\colon A \to B + C$ be a homomorphism of Abelian groups such that the composition $A \to B + C \to B + C/C$ is an isomorphism. Then f is a monomorphism onto a direct summand.*

The proof is elementary.

Since $\mathfrak{H}_\#\eta''$ is an isomorphism in (4.8), so is $\eta'\mathfrak{H}$; and since η' is the projection onto a direct summand, by (4.9), $\mathfrak{H}$ is a monomorphism onto a direct summand for $s \leqq n+1$. Suspending $X \mathbf{X} X$ and using ϕ, one obtains (4.3).

We now proceed to the computation of the elements a^{i+1}, described in (4.5). The identification map $X \times X \to X \mathbf{X} X$ induces isomorphisms $H_{2n+s+1}(X \times X, X \vee X) \approx H_{2n+s+1}(X \mathbf{X} X)$ for all s and $\pi_{2n+s+1}(X \times X, X \vee X) \approx \pi_{2n+s+1}(X \mathbf{X} X)$ for $s \leqq n$. It suffices therefore to compute the corresponding element $a^{i+1}(X \mathbf{X} X) \in H^{i+1}(X \mathbf{X} X); \pi_{i+1}(X \mathbf{X} X))$ such that $\alpha(a^{i+1})$ is a left-inverse for $\mathfrak{H}$.

In the Künneth formula,

$$H_{2n+s+1}(X \mathbf{X} X) \approx \sum_{\substack{i+j=2n+s+1\\ i,j>0}} H_i(X) \otimes H_j(X) + \sum_{\substack{i+j=2n+s\\ i,j>0}} H_i(X) * H_j(X)$$

the embedding of the torsion term $H_i(X) * H_j(X)$ is only well-defined modulo $H_{i+1}(X) \otimes H_j(X) + H_i(X) \otimes H_{j+1}(X)$ ([6], § 12). Since $H_{n+2}(X) = 0$, $H_{2n+s+1}(X \mathbf{X} X)$ splits into two natural direct summands.

$$G = H_{n+1}(X) \otimes H_{n+s}(X) + H_{n+1}(X) * H_{n+s-1}(X),$$

and the sum of the remaining terms. The homomorphism $\mathfrak{H}\colon \pi_{2n+s+1}(X \boldsymbol{\times} X) \to H_{2n+s+1}(X \boldsymbol{\times} X)$ composed with the projection onto G is an isomorphism. Hence, if an element $a \in H^{2n+s+1}(X \boldsymbol{\times} X; \pi_{2n+s+1}(X \boldsymbol{\times} X))$ be found such that $\alpha(a) \in \operatorname{Hom}(H_{2n+s+1}(X \boldsymbol{\times} X); \pi_{2n+s+1}(X \boldsymbol{\times} X))$ is an isomorphism on G and 0 on the other summand, then $\alpha(a)$ is, up to coefficient isomorphism, a left-inverse for $\mathfrak{H}$. Since we are calculating modulo coefficient isomorphism, we may replace $\pi_{2n+s+1}(X \boldsymbol{\times} X)$ by G.

Let π be finitely-generated, $\pi = \sum A(u_i)$, where u_i is a generator of $A(u_i) = Z$ or Z_{p^f}, p a prime. We shall see that it suffices to calculate a certain element $a(i,j)$ for each pair (i,j), and to add all $a(i,j)$ in order to obtain a. The notation in the following diagram will be explained in the various cases:

$$\begin{tikzcd}
H^{2n+s+1}(K' \boldsymbol{\times} K''; G_{ab}) \arrow[r, "\alpha"] \arrow[dd, "\lambda_{p*}"'] \arrow[dr, "\alpha'"] & \operatorname{Hom}(H_{2n+s+1}(K' \boldsymbol{\times} K''); G_{ab}) \\
 & \operatorname{Hom}(H_{2n+s+1}(K' \boldsymbol{\times} K''; Z_p); G_{ab}) \arrow[u, "\operatorname{Hom}(\lambda_p, 1)"'] \arrow[d, "\operatorname{Hom}(1, \lambda_p)"'] \\
H^{2n+s+1}(K' \boldsymbol{\times} K''; G'_{ab}) \arrow[r, "\alpha''"] & \operatorname{Hom}(H_{2n+s+1}(K' \boldsymbol{\times} K''; Z_p), G'_{ab})
\end{tikzcd}$$

We restrict s to $3 \leqq s \leqq n$, and use without further reference the results of [4], § 5.

Case 1.

$$K' = K(Z_{p^a}, n+1), \qquad K''(Z_{p^b}, n+1),$$

$$G_{ab} = H_{n+1}(K') \otimes H_{n+s}(K'') + H_{n+1}(K') * H_{n+s-1}(K'').$$

λ_p denotes reduction modulo p and the induced homomorphism on homology groups. $H_{2n+s+1}(K' \boldsymbol{\times} K'')$ is a Z_p-vector space; it is mapped by λ_p isomorphically onto a direct summand of $H_{2n+s+1}(K' \boldsymbol{\times} K''; Z_p)$, while G_{ab} is mapped isomorphically onto the direct summand $G'_{ab} = H_{n+1}(K'; Z_p) \otimes H_{n+s}(K''; Z_p)$ by $\Lambda_p = \eta\lambda_p$, where η is the projection onto G'_{ab}. $\operatorname{Hom}(1, \Lambda_p)$ is an isomorphism, and so is the homomorphism Λ_{p*} induced by Λ_p. The homomorphisms α, α', α'' are given by the universal coefficient theorems. The required element a is $\Lambda_{p*}^{-1}(a')$, where $a' \in H^{2n+s+1}(K' \boldsymbol{\times} K''; G'_{ab})$ is such that $\alpha''(a')$ is the projection onto G'_{ab}. Let $b' \in H^{n+1}(K'; Z_p)$ be the image of the basic class under reduction modulo p, and similarly for b''. Now $H_{n-s}(K''; Z_p) = \sum Z_p(J)$, where $Z_p(J) \approx Z_p$ and the Steenrod homology operation $St^p{}_J$ maps $Z_p(J)$ isomorphically onto $H_{n+1}(K''; Z_p)$ and vanishes on the other summands ($St^p{}_J$ is the dual of $St^J{}_p = St^I{}_p$ or $St^{I,b}{}_p$ in the notation of Cartan). Hence we may take $a' = b' \times \sum St^J{}_p b''$, where the sum is taken over the Cartan basis of $H^{n+s}(K''; Z_p)$, $St^J{}_p b''$ has coefficients in $Z_p(J)$, and the pairing for the cross-product is the natural map

$$Z_p \otimes Z_p(J) \rightarrow H_{n+1}(K'; Z_p) \otimes H_{n+s}(K''; Z_p) = G_{ab}.$$

Case 2. $K' = K(Z_{p^a}, n+1)$, $K'' = K(Z, n+1)$. The discussion for this case is identical with the preceding one, except that no operations of type $St^{I,b}{}_p$ occur.

Case 3.

$$K' = K(Z, n+1),\ K'' = K(Z_{p^b}, n+1),\ G_{ab} = H_{n+1}(K') \otimes H_{n+s}(K'').$$

$H_{2n+s+1}(K' \mathbf{X} K'')$ is again a Z_p-vector space; λ_p maps G_{ab} isomorphically onto the direct summand $G'_{ab} = H_{n+1}(K'; Z_p) \otimes \bar{H} \subset H_{n+1}(K'; Z_p) \otimes H_{n+s}(K''; Z_p)$, where $\bar{H}$ is the subspace of $H_{n+s}(K''; Z_p)$ generated by elements corresponding to those $St^p{}_J$ such that the dual $St^J{}_p = St^I{}_p$ or $St^{I,b}{}_p$ corresponds to a sequence $I = (a_0, \cdots, a_k)$ with $a_k \equiv 0\,(2p-2)$. We may therefore take $a' = b' \times \sum St^J{}_p b''$, where $St^J{}_p b''$ has coefficients in $Z_p(J) \subset \bar{H}$, the sum is taken over those elements of the basis for $H^{n+s}(K''; Z_p)$ which do not end in a Bockstein operator, and the pairing of coefficients is the same as in case 1.

Case 4. $K' = K'' = K(Z, n+1)$, $G_{ab} = H_{n+1}(K') \otimes H_{n+s}(K'')$. Here $H_{2n+s+1}(K' \mathbf{X} K'')$ is a torsion group, and its p-primary component $H_{2n+s+1}(K' \mathbf{X} K'')_p$ is a Z_p-vector space; λ_p maps it isomorphically onto a direct summand of $H_{2n+s+1}(K' \mathbf{X} K''; Z_p)$, and $(G_{ab})_p$ isomorphically onto the direct summand G'_{ab}, as in case 3. In order to find an element a such that $\alpha(a)$ is a projection onto G_{ab}, it suffices to find, for each prime p such that $H_{n+s}(Z, n+1)_p \neq 0$, an element a'_p such that $\alpha''(a'_p)$ is a projection onto G'_{ab}. As in case 3, such an element is given by $a'_p = b' \times \sum St^I{}_p b''$, where $St^I{}_p$ has coefficients in $Z_p(I)$, and the sum is taken over those elements of the basis for $H^{n+s}(K''; Z_p)$ which do not end with a Bockstein operator.

We conclude the computation by combining the various cases considered above. If A, A' are Abelian groups,

$$H_r(A + A', n+1) = H_r(A, n+1) + H_r(A', n+1)$$

for $r \leqq 2n+1$; hence, the group $H_{2n+s+1}(X \mathbf{X} X)$ is a bilinear function of the summands $A(u_i)$ of π. In order to calculate the required element a, we therefore need only consider pairs $A(u_i)$, $A(u_j)$ of summands, and calculate the corresponding $a(i, j)$ as above.

Applying (4.5) and the above computation, we obtain the following. Let $\eta_i: \pi \rightarrow A(u_i)$ be the projection, b_i the reduction modulo p (where p is the appropriate prime in each case) of $\eta_{i*}b \in H^{n+1}(E_{2n+s-1}, A(u_i))$, where b is the basic class in E_{2n+s-1}.

(4.10) THEOREM.

$$-k^{2n+s+1}(SK(\pi, n)) \in H^{2n+s+1}(E_{2n+s-1}; G), \qquad 3 \leqq s \leqq n,$$

is the sum of the following terms, indexed by ordered pairs (u_i, u_j) *of generators, not necessarily distinct, in which* (a) *the operations* $St^J{}_p$ *for the case* (i, j) *has coefficient group* $Z_p(i, j, J) = Z_p$, *and the coefficient groups with different indexing sets are distinct*; (b) *the cup-product pairings are all isomorphisms*; (c) G *is the direct sum of the coefficient groups for the various terms*:

(1) *If* u_i *and* u_j *have orders which are powers of the same prime, say* p^a *and* p^b *respectively: a term* $b_i \cup \sum St^J{}_p b_j$, *where* $\{St^J{}_p\}$ *is the basis for* $H^{n+s}(Z_{p^b}, n+1; Z_p)$.

(2) *If* u_i, u_j *have orders* p^a, ∞ *respectively: a term* $b_i \cup \sum St^I{}_p b_j$, *where* $\{St^I{}_p\}$ *is the basis for* $H^{n+s}(Z, n+1; Z_p)$.

(3) *If* u_i, u_j *have orders* ∞, p^b *respectively: a term* $b_i \cup \sum St^J{}_p b_j$, *where* $\{St^J{}_p\}$ *is the set of those elements of the basis for* $H^{n+s}(Z_{p^b}, n+1; Z_p)$ *which do not end in a Bockstein operator.*

(4) *If both* u_i, u_j *have order* ∞: *for each prime* p *such that* $H_{n+s}(Z, n+1)_p \neq 0$, *a term* $b_i \cup \sum St^I{}_p b_j$, *where* $\{St^I{}_p\}$ *is the set of those elements of the basis for* $H^{n+s}(Z, n+1; Z_p)$ *which do not end in a Bockstein operator.*

In the case $s = 2$, $H_{2n+s+1}(X \times X)$ is a torsion group, but the p-primary component is no longer a Z_p-vector space. For this case, let $b_i = \eta_{i*}b$, without reducing modulo p. Then, by a simple direct argument, we have

(4.11) THEOREM. $-k^{2n+3}(SK(\pi, n)) = \sum \theta_i b_i \cup \theta_j b_j \in H^{2n+3}(E_{2n+1}; G)$, *where* (a) *the summation is over those pairs of generators* u_i, u_j *whose orders are powers of the same prime, say* p^a, p^b *respectively*; (b) $\theta_i = 1, \delta_{p^a}, \delta_{p^a}$; $\theta_j = \delta_{p^b}, 1, 1$, *according as* $a < b$, $a > b$, $a = b$, *where* $\delta_{p^k}: H^{n+1}(K; Z_{p^k}) \rightarrow H^{n+2}(K; Z_{p^k})$ *is the Bockstein operator*; (c) *the coefficient pairing* $A(u_i) \otimes A(u_j) \rightarrow A(u_i) * A(u_j)$ *is an isomorphism*; (d) $G = \sum A(u_i) * A(u_j)$.

BROWN UNIVERSITY AND THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] J. F. Adams, "Four applications of the self-obstruction invariants," *The Journal of the London Mathematical Society*, vol. 31 (1956), pp. 148-159.

[2] A. L. Blakers and W. S. Massey, "Products in homotopy theory," *Annals of Mathematics*, vol. 58 (1953), pp. 295-324.

[3] R. Bott and H. Samelson, "On the Pontrjagin product in spaces of paths," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 320-337.

[4] H. Cartan, "Sur les groupes d'Eilenberg-MacLane, II," *Proceedings of the National Academy of Sciences*, vol. 40 (1954), pp. 704-707.

[5] H. Cartan and J.-P. Serre, "Espaces fibrés et groupes d'homotopie I et II," *Comptes Rendus de l'Académie des Sciences*, vol. 234 (1952), pp. 288 and 293.

[6] S. Eilenberg and S. MacLane, "On the groups $H(\pi, n)$, II," *Annals of Mathematics*, vol. 60 (1954), pp. 49-139.

[7] I. M. James, "On the suspension triad," *Annals of Mathematics*, vol. 63 (1956), pp. 191-247.

[8] J.-P. Meyer, "Whitehead products and Postnikov systems" (to appear).

[9] J. W. Milnor, "On spaces having the homotopy type of a *CW* complex," *Transactions of the American Mathematical Society* (to appear).

[10] J. C. Moore, "Some applications of homology theory to homotopy problems," *Annals of Mathematics*, vol. 58 (1953), pp. 325-350.

[11] ———, *Semi-simplicial complexes and Postnikov systems*, Princeton (1956) (mimeographed).

[12] ———, "On the homology of $K(\pi, n)$," *Proceedings of the National Academy of Sciences*, vol. 43 (1957), pp. 409-411.

[13] M. M. Postnikov, *Doklady Akademii Nauk S.S.S.R.*, vol. 76 (1951), pp. 359-362 and 789-791; *ibid.*, vol. 79 (1951), pp. 573-576.

[14] J.-P. Serre, "Homologie singulières des espaces fibrés," *Annals of Mathematics*, vol. 54 (1951), pp. 425-505.

[15] ———, "Groupes d'homotopie et classes de groupes Abéliens," *ibid.*, vol. 58 (1953), pp. 258-294.

[16] H. Suzuki, "On the Eilenberg-MacLane invariants of loop spaces," *Journal of the Mathematical Society of Japan*, vol. 8 (1956), pp. 93-101.

[17] G. W. Whitehead, "On the Freudenthal theorems," *Annals of Mathematics*, vol. 57 (1954), pp. 209-228.

[18] ———, "On the homology suspension," *ibid.*, vol. 62 (1955), pp. 254-268.

[19] ———, "Homotopy groups of joins and unions," *Transactions of the American Mathematical Society*, vol. 83 (1956), pp. 55-69.

AN INTERPOLATION PROBLEM FOR BOUNDED ANALYTIC FUNCTIONS.*

By LENNART CARLESON.

1. In a classical paper [4], R. Nevanlinna has given a necessary and sufficient condition that the interpolation

$$f(z_\nu) = w_\nu, \qquad \nu = 1, 2, \cdots, \tag{1.1}$$

be possible for a given sequence of points $\{z_\nu\}$, $|z_\nu| < 1$, and an analytic function $f(z)$ in $|z| < 1$, $|f(z)| \leqq 1$. The result is, however, very implicit and gives in a concrete situation very little help in deciding if the interpolation is possible or not.

The object of the present paper is to give a simple and explicit condition on $\{z_\nu\}$ under which the interpolation (1.1) is possible with a bounded function $f(z)$. If we allow $\{w_\nu\}$ to be an arbitrary bounded sequence, the condition is also a necessary one. It should be observed that even the existence of *any* infinite such sequence $\{z_\nu\}$ is non-trivial; this problem was suggested by R. C. Buck and constructions of such examples have also recently been given by Gleason and Newman (unpublished).

The proof of the main theorem depends on a reformulation of problem (1.1) which is presented in section 2. It is essentially included in a result by Garabedian [2]; since the discussion there is quite general and the proof complicated, we have included a complete and simple proof here. Section 3 contains an inequality of the Schwarz type, which is the crucial step in our proof. This is then completed in section 4. The last section is devoted to an application to the ideal structure in the algebra of bounded analytic functions.

2. Let $z_1, z_2, \cdots, z_n$ be a sequence of different complex numbers, $0 < |z_\nu| < 1$, and let $w_1, w_2, \cdots, w_n$ be arbitrary complex numbers. Let H^q, $q \geqq 1$, be the Banach space of functions $f(z)$ analytic in $|z| < 1$ under the norm

$$\| f \|_q = \lim_{r \to 1} \{ \tfrac{1}{2\pi} \int_{-\pi}^{\pi} | f(re^{i\theta}) |^q \, d\theta \}^{1/q}.$$

---

* Received March 26, 1958.

We consider the extremal problem

$$\inf_{f \in H^q} \| f \|_q = m_q \tag{2.1}$$

under the conditions

$$f(z_\nu) = w_\nu, \qquad \nu = 1, \cdots, n. \tag{2.2}$$

It is obvious that the lower bound m_q is assumed for a (unique) function $f_q \in H^q$. If $\pi_n(z)$ is a Blaschke product corresponding to the sequence $\{z_\nu\}$,

$$\pi_n(z) = \prod_1^n (z - z_\nu)/(1 - z\bar{z}_\nu), \tag{2.3}$$

then any function in H^q satisfying conditions (2.2) has the form $f = f_q + \eta\pi_n \cdot g$, $g \in H^q$. If η is an arbitrary (small) complex number, a standard variation yields

$$\int_{|z|=1} | f_q |^{q-2} \bar{f}_q \pi_n g \, d\theta = 0, \qquad g \in H^q. \tag{2.4}$$

If we choose for $g(z)$ the functions z^p, $p = 0, 1, \cdots$, the well-known Riesz theorem shows that there is a function $F_q(z) \in H^1$ with boundary values a.e. on $| z | = 1$ such that

$$F_q = | f_q |^{q-2} \bar{f}_q \pi_n z^{-1} m_q^{1-q}. \tag{2.5}$$

If we use the boundary values (2.5), Hölder's inequality yields

$$\| F_q \|_1 \leqq 1. \tag{2.6}$$

We now observe that by Cauchy's integral formula, we have

$$m_q = \tfrac{1}{2\pi} m_q^{1-q} \int_{|z|=1} | f_q |^q \, d\theta = \tfrac{1}{2\pi i} \int_{|z|=1} (F_q \cdot f_q / \pi_n) \, dz = \sum_1^n F_q(z_\nu) \cdot w_\nu / \pi'_n(z_\nu). \tag{2.7}$$

We now let $q \to \infty$. By (2.1) and (2.6), we can select a subsequence so that the corresponding sequences $f_q(z)$ and $F_q(z)$ converge to limit functions, $f(z)$ and $F(z)$, which still satisfy conditions (2.2) resp. (2.6). $f(z)$ is also bounded and satisfies (2.2) with the least possible maximum m_∞. If $G(z)$ is an arbitrary function in H^1, $\| G \|_1 \leqq 1$, then by Cauchy's formula,

$$| \sum_1^n G(z_\nu) w_\nu / \pi_n'(z_\nu) | = | \tfrac{1}{2\pi i} \int_{|z|=1} G f \pi_n^{-1} \, dz | \leqq m_\infty \| G \|_1 \leqq m_\infty. \tag{2.8}$$

On the other hand, if we let $q \to \infty$ in (2.7), we have equality in (2.8). Hence the following theorem is proved.

THEOREM 1. *Let* m_∞ *be the least possible maximum of an analytic function in* $|z| < 1$ *satisfying conditions* (2.2). *Then*

$$m_\infty = \sup_{\|G\|_1=1} \left| \sum_1^n G(z_\nu) w_\nu / \pi_n'(z_\nu) \right|. \tag{2.9}$$

3. We shall in this section prove an auxiliary result of some independent interest. It is related to a well-known theorem by Hardy and Littlewood, see [3], p. 291. We use the letter A to denote absolute constants.

THEOREM 2. *Let* σ_ν *be a sequence of open subintervals of* $(0,1)$. *Denote by* σ_ν' *the interval obtained from* σ_ν *by adjoining to* σ_ν *equally long intervals on both sides, and let the length of* σ_ν *be* l_ν. *Then the conditions*

$$\sum_{\sigma_j \subset \sigma_i'} l_j \leqq C \cdot l_i \tag{3.1}$$

for all i *and a fixed constant* C, *imply*

$$\sum_{\nu=1}^{\infty} (1/l_\nu) \left(\int_{\sigma_\nu} f(x)\,dx \right)^2 \leqq A \cdot C \int_0^1 f(x)^2 dx, \tag{3.2}$$

for all square integrable functions f.

We first reduce our theorem to the case when all σ_ν have the form $(k2^{-n}, (k+1)2^{-n})$, where k and n are integers. Every σ_ν is included in the union of at most four equally long intervals of this form of length $< \frac{1}{2} l_\nu$. Let ω_i be the intervals thus obtained and let m_i be the length of ω_i. Condition (3.1) implies

$$\sum_{\omega_j \subset \omega_i} m_j \leqq 4C m_i = c m_i, \tag{3.3}$$

and it is sufficient to prove that (3.3) implies that (3.2) holds with σ and l replaced by ω and m.

Let $\chi_\nu(x)$ be the characteristic function of ω_ν and introduce the kernel

$$K(x,y) = \sum_1^\infty \chi_\nu(x) \chi_\nu(y) / m_\nu.$$

We have the inequality, $f > 0$,

$$\begin{aligned} \sum_1^\infty (1/m_\nu) \left(\int_{\omega_\nu} f(x)\,dx \right)^2 &= \int_0^1 f(x)\,dx \int_0^1 K(x,y) f(y)\,dy \\ &\leqq \left\{ \int_0^1 f(x)^2 dx \right\}^{\frac{1}{2}} \left\{ \int_0^1 dx \left(\int_0^1 K(x,y) f(y)\,dy \right)^2 \right\}^{\frac{1}{2}}. \end{aligned} \tag{3.4}$$

The last factor can be written, $m_{ij} = m(\omega_i \cap \omega_j)$, as the square root of

$$(3.5) \qquad F(x,x) = \sum_{i,j} (m_{ij}/\sqrt{m_i}\sqrt{m_j}) x_i x_j,$$

where $x_i = (1/\sqrt{m_i}) \int_{\omega_i} f,x) dx$. If we can prove that the quadratic form $F(x,x)$ has a bound $AC \sum_1^\infty x_i^2$, our theorem follows from (3.4).

To be able to discuss the form (3.5), we must carry out the summation in a special way. We say that the index i belongs to the first generation G_1 if ω_i is not included in any larger interval ω_j; if there are several equal intervals, we choose anyone of them as defining a member of the first generation. The second generation G_2 is defined as the collection of first generations corresponding to the intervals associated with G_1. This can evidently be continued until all intervals are exhausted. Similarly, if ω_i is a fixed interval with i belonging to G_k, $G_{i\nu}$, $\nu = 0, 1, 2, \cdots$, denotes the members of $G_{\nu+k}$ corresponding to the subinterval of ω_i.

Let a_ν be the total length of the intervals corresponding to $G_{i\nu}$ for some i. The inequalities (3.3) and our construction imply $(a_0 = m_i)$

$$(3.6) \qquad \sum_{\nu=n}^{\infty} a_\nu \leqq c a_n, \qquad n = 0, 1, \cdots$$

$$(3.7) \qquad a_0 \geqq a_1 \geqq a_2 \geqq \cdots \geqq 0.$$

These conditions are sufficient for an explicit estimate of a_ν which is contained in the following lemma.

LEMMA 1. *Let* $c \geqq 2$ *be a positive integer. The conditions* (3.6) *and* (3.7) *imply*

$$(3.8) \qquad a_n \leqq 4(1 - (1/c))^n a_0.$$

Let $N > c$ be a fixed index and let $\{a_\nu\}$ be a sequence which maximizes a_N under the conditions (3.6), (3.7) and $a_0 = 1$. Evidently $a_n = 0$, $n > N$, and $a_n = a_N$, $N \geqq n > N - c$. For $n \leqq N - c$, a_n is defined by recursion,

$$\sum_{\nu=n}^{N} a_\nu = c a_n, \qquad n \leqq N - c,$$

which yields $(a_0 = 1)$ $a_n = (1 - (1/c))^n$. Hence

$$a_N \leqq a_{N-c} = (1 - (1/c))^N (1 - (1/c))^{-c} < 4(1 - (1/c))^N,$$

which was our assertion.

We can now complete the proof of Theorem 2. For the quadratic form $F(x,x)$ of (3.5), we have the estimate

$$F(x,x)^2 \leqq 4 \cdot \sum_1^\infty x_i^2 \cdot \sum_{i=1}^\infty (1/m_i) \Big(\sum_{\nu=0}^\infty \sum_{j \in G_{i\nu}} \sqrt{m_j}\, x_j \Big)^2.$$

We define $k > 0$ by $k^2 = 1 - (1/4C)$ and find for the last factor, by Schwarz' inequality and the lemma, the estimate

$$\begin{aligned} &\sum_{i=1}^\infty (1/m_i) \sum_{\nu=0}^\infty k^{-\nu} \Big(\sum_{j \in G_{i\nu}} \sqrt{m_j}\, x_j \Big)^2 \cdot \sum_0^\infty k^\nu \\ &\qquad \leqq 1/(1-k) \sum_{i=1}^\infty (1/m_i) \sum_{\nu=0}^\infty k^{-\nu} \sum_{j \in G_{i\nu}} m_j \cdot \sum_{j \in G_{i\nu}} x_j^2 \\ &\qquad \leqq 4/(1-k) \sum_{\mu=1}^\infty \sum_{i \in G_\mu} \sum_{\nu=0}^\infty k^\nu \sum_{j \in G_{i\nu}} x_j^2 = 4/(1-k) \sum_{\mu=1}^\infty \sum_{\nu=0}^\infty k^\nu \sum_{j \in G_{\mu+\nu}} x_j^2 \\ &\qquad \leqq 4/(1-k) \sum_{j=1}^\infty x_j^2 \cdot \sum_{\nu=0}^\infty k^\nu = (4/(1-k)^2) \sum_1^\infty x_i^2. \end{aligned}$$

The definition of k now shows that $(1-k)^{-2} \leqq A^2C^2$ and our theorem is proved.

4. We can now prove our main theorem.

THEOREM 3. *Let* $\{z_\nu\}$ *be a sequence of complex numbers,* $0 < |z_\nu| < 1$. *Then the interpolation problem*

$$(4.1) \qquad f(z_\nu) = w_\nu, \quad f(z) \text{ bounded analytic in } |z| < 1,$$

is solvable for arbitrary bounded w_ν *if and only if*

$$(4.2) \qquad \prod_{\nu \neq \mu} |(z_\nu - z_\mu)/(1 - z_\nu \bar{z}_\mu)| \geqq \delta > 0, \qquad \mu = 1, 2, \cdots.$$

Remark. If $[z_\nu, z_\mu]$ denotes the hyperbolic distance between z_ν and z_μ the necessary and sufficient condition for an arbitrary simply-connected domain reads:

$$(4.2.\text{a}) \qquad \prod_{\nu \neq \mu} \operatorname{tgh}(2[z_\nu, z_\mu]) \geqq \delta > 0.$$

For the proof of the necessity we need the following simple lemma.

LEMMA 2. *Let* $|a| < 1$ *be a fixed complex number. Then*

$$(4.3) \qquad \sup_\phi |\phi(a)| = 1/(1 - |a|^2), \qquad \|\phi\|_1 \leqq 1.$$

When discussing the upper bound (4.3), we may assume $\phi(z) \neq 0$ and set $\sqrt{\phi} = \psi(z)$,

$$\psi(z)=\sum_0^\infty c_\nu z^\nu, \qquad \sum_0^\infty |c_\nu|^2\leqq 1.$$

Hence

$$|\phi(a)|=|\psi(a)|^2\leqq\sum_0^\infty|c_\nu|^2\cdot\sum_0^\infty|a|^{2\nu}\leqq 1/(1-|a|^2)$$

with equality for $\phi(z)=(1-|a|^2)/(1-\bar{a}z)^2$.

Let us now assume that every problem (4.1) is solvable. Consider all f satisfying (4.1) and define a norm in the space of bounded sequence $\{w_\nu\}=w$ by

$$N(w)=\inf_f \sup_{|z|<1}|f(z)|$$

for such f's. The space of w's is a Banach space under this norm which implies

$$N(w)\leqq \text{Const.} \sup_\nu |w_\nu|.$$

Theorem 1 then yields

$$(4.4) \qquad \sum_{\nu=1}^n |G(z_\nu)/\pi_n'(z_\nu)|\leqq \text{Const.}, \qquad \|G\|_1\leqq 1.$$

If we choose for G the function ϕ which by Lemma 2 belongs to the point z_μ, we find in particular

$$(4.5) \qquad (1-|z_\mu|^2)|\pi_n'(z_\mu)|=\prod_{\substack{\nu\neq\mu\\ \nu\leqq n}}|(z_\nu-z_\mu)/(1-z_\nu\bar{z}_\mu)|\geqq\delta>0,$$

which was our assertion.

For the converse, it is necessary to prove that (4.4) holds. By (4.5), this is equivalent to the statement

$$(4.6) \qquad \sum_{\nu=1}^\infty (1-|z_\nu|^2)|G(z_\nu)|\leqq \text{Const.}, \qquad \|G\|_1\leqq 1.$$

In proving (4.6), we need only consider functions $G(z)$ in H^1 which do not vanish in $|z|<1$. We may thus replace G in (4.6) by ϕ^2, $\phi\in H^2$. If, finally, $u(z)$ is the real part of ϕ, we need only prove

$$(4.7) \qquad \sum_1^\infty (1-|z_\nu|^2)u(z_\nu)^2\leqq \text{Const.}, \quad \frac{1}{2\pi}\int_{-\pi}^{\pi}u(re^{i\theta})^2\,d\theta\leqq 1,$$

for positive harmonic function u.

Let $f(\theta)>0$ be the boundary values of $u(re^{i\theta})$, $f\in L^2(-\pi,\pi)$. We change the definition of f by defining $f(\theta)\equiv 0$, $|\theta|>2\pi$. Simple estimates of the Poisson kernel show that

$$u(z_\nu) \leqq A \sum_{0}^{\infty} (1/4^n\alpha_\nu) \int_{-2^n\alpha_\nu}^{2^n\alpha_\nu} f(\theta+\theta_\nu)\,d\theta, \qquad z_\nu = (1-\alpha_\nu)e^{i\theta_\nu}.$$

By Schwarz's inequality,

$$(4.8) \qquad \alpha_\nu u(z_\nu)^2 \leqq A \sum_{0}^{\infty} (1/5^n)(1/2^{n+1}\alpha_\nu)\Big(\int_{\sigma_\nu^{(n)}} f(\theta)\,d\theta\Big)^2,$$

where $\sigma_\nu = \sigma_\nu^{(n)}$ denotes the part of the interval $|\theta - \theta_\nu| < 2^n\alpha_\nu$ which belongs to $(-2\pi, 2\pi)$. To prove Theorem 3 it is, by Theorem 2, sufficient to prove that the intervals $\sigma_\nu^{(n)}$ satisfy the conditions (3.1) with a constant C not exceeding $A4^n$.

Since

$$|(z_\nu - z_\mu)/(1 - z_\nu\bar{z}_\mu)|^2 = 1 - (1 - |z_\nu|^2)(1 - |z_\mu|^2)/|1 - z_\nu\bar{z}_\mu|^2,$$

our assumption (4.2) implies

$$\alpha_\nu \sum_{\mu=1}^{\infty} \alpha_\mu/|1 - z_\nu\bar{z}_\mu|^2 \leqq \text{Const.}, \qquad \nu = 1, 2, \cdots,$$

which yields

$$(4.9) \qquad \alpha_\nu \sum_{3\alpha_\nu \geqq \alpha_\mu} \alpha_\mu/(\alpha_\nu^2 + (\theta_\nu - \theta_\mu)^2) \leqq \text{Const.}, \qquad \nu = 1, 2, \cdots.$$

We now distinguish two cases. If $\sigma_\nu' = (-2\pi, 2\pi)$, in which case $\alpha_\nu > (2\pi/3)2^{-n}$, we find for the left hand side of (3.1) the estimate

$$\sum_{\alpha_\mu > 2^{-n}} 4\pi + \sum_{\alpha_\mu \leqq 2^{-n}} 2^{n+1}\alpha_\mu \leqq A2^n \leqq (A2^n)(2^{n+1}\alpha_\nu).$$

If σ_ν' is a proper sub-interval of $(-2\pi, 2\pi)$, the estimate (4.9) shows that

$$\sum_{\sigma_\mu \subset \sigma_\nu'} 2^{n+1}\alpha_\mu \leqq A4^n \cdot 2^{n+1}\alpha_\nu.$$

Hence (3.1) holds with $C = A4^n$ and the proof is complete.

5. The method used in section 2 together with Theorem 3 give us the possibility of studying the ideal structure of the Banach algebra B of bounded analytic functions in $|z| < 1$ under the usual norm $\|f\| = \sup_{|z|<1} |f(z)|$.

Let $f(z)$ and $g(z)$ be two functions in the Banach algebra C of functions analytic and uniformly continuous in $|z| < 1$. It is an easy consequence of Gelfand's theory on maximal ideals (compare also [1]) that the closed ideal generated by f and g is C if and only if

$$(5.1) \qquad |f(z)| + |g(z)| \geqq \delta > 0, \qquad |z| < 1.$$

Under this condition, there exist coefficients $a(z)$, $b(z)$ in C so that

$$af + bg = 1, \qquad |z| < 1. \tag{5.2}$$

We consider the equation (5.2) for all pairs (a, b) of functions in H^q and study the variational problem

$$\inf\{\|a\|_q^q + \|b\|_q^q\} = m_q^q. \tag{5.3}$$

Let (a_q, b_q) be a minimizing pair, and consider the variation $(a_q + \eta hg$, $b_q - \eta hf)$, $h \in H^q$, for small complex numbers η. As above, we find that

$$(|a_q|^{q-2}\bar{a}_q g - |b_q|^{q-2}\bar{b}_q f) = F_q, \qquad |z| = 1, \tag{5.4}$$

where $F_q \in H^1$ and $F_q(0) = 0$. Let ϕ be an arbitrary function in C. (5.4) together with $a_q f + b_q g = 1$ yields

$$\begin{aligned} 1/2\pi \int_{|z|=1} m_q^{-q}(|a_q|^q + |b_q|^q) g\phi\, |dz| &= (1/2\pi m_q) \int_{|z|=1} |b_q|^{q-2}\bar{b}_q\phi\, |dz|, \\ 1/2\pi \int_{|z|=1} m_q^{-q}(|a_q|^q + |b_q|^q) f\phi\, |dz| &= (1/2\pi m_q) \int_{|z|=1} |a_q|^{q-2}\bar{a}_q\phi\, |dz|. \end{aligned} \tag{5.5}$$

We now let $q \to \infty$. m_q then tends to m, the least possible maximum for coefficients (a, b) satisfying (5.2). After a selection, the formulas (5.5) become

$$\begin{aligned} \int_{|z|=1} g\phi\, dp &= (1/m) \int_{|z|=1} \phi\, d\beta, \\ \int_{|z|=1} f\phi\, dp &= (1/m) \int_{|z|=1} \phi\, d\alpha, \end{aligned} \tag{5.6}$$

where p, α and β have the following properties

$$dp \geqq 0, \int_{|z|=1} dp = 1, \int_{|z|=1} |d\alpha| \leqq 1, \int_{|z|=1} |d\beta| \leqq 1. \tag{5.7}$$

The formulas (5.6) and (5.7) permit us to prove the following theorem.

THEOREM 4. *Let $\pi(z)$ be a Blaschke product with zeros z_ν and let $f(z)$ be an arbitrary function in B such that $|f(z)| + |\pi(z)| \geqq \delta > 0$ in $|z| < 1$. Then*

$$af + b\pi = 1 \tag{5.8}$$

is solvable with coefficients a and b in B if and only if the interpolation

$$a(z_\nu) = 1/f(z_\nu), \qquad \nu = 1, 2, \cdots, a \in B, \tag{5.9}$$

is possible. (5.8) *is thus solvable if* (4.2) *holds.*

The condition (5.9) is obviously necessary. Let us assume that (5.9) holds and consider the pair of functions in C

$$f_n(z) = f(r_n z), \quad r_n < 1, \quad g_n(z) = \prod_1^n (z - z_\nu)/(1 - z\bar{z}_\nu).$$

If r_n is sufficiently close to 1, the interpolation problem $h_n(z_\nu) = f_n(z_\nu)^{-1}$, $\nu = 1, 2, \cdots, n$, has a solution $h_n(z) \in C$, $|h_n(z)| \leqq M$, M independent of n. Let p_n, α_n, β_n be the function of (5.6) and (5.7) associated with f_n and g_n, and let m_n be the corresponding constant m. Our theorem follows if we can prove that

$$m_n = O(1), \qquad n \to \infty. \tag{5.10}$$

Let C_n be the closed linear subspace of C of functions vanishing at $z_1, z_2, \cdots, z_n$. Every function $\phi \in C_n$ has the form $\phi = g_n \cdot \psi$, $\| \phi \| = \| \psi \|$. We define a linear functional $L_n(\phi)$ on C_n:

$$L_n(\phi) = \int_{|z|=1} \phi \, dp_n = (1/m_n) \int_{|z|=1} \psi \, d\beta_n, \qquad \phi \in C_n. \tag{5.11}$$

It follows that $\| L_n \| \leqq 1/m_n$. By the Hahn-Banach theorem, $L_n(\phi)$ can be extended to C so that

$$|L_n(\phi)| \leqq (1/m_n) \| \phi \|, \qquad \phi \in C. \tag{5.12}$$

On the other hand, if $l_n(\phi)$ is the linear functional defined by the first equation of (5.11) for *all* $\phi \in C$, we obviously have for certain constants λ_ν

$$L_n(\phi) - l_n(\phi) = \sum_1^n \lambda_\nu \phi(z_\nu). \tag{5.13}$$

Choosing $\phi \equiv 1$ we find

$$\left| \sum_1^n \lambda_\nu \right| \geqq 1 - (1/m_n);$$

if, however, we choose $\phi = h_n f_n$, $\phi(z_\nu) = 1$, $\nu = 1, 2, \cdots, n$, while the second formula (5.6) yields

$$1 - (1/m_n) \leqq \left| \sum_1^n \lambda_\nu \right| \leqq (1/m_n)(\| h_n \| \cdot \| f_n \| + \| h_n \|) \leqq (M/m_n)(1 + \| f \|).$$

This inequality proves (5.10) and the proof is complete.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
AND
UNIVERSITY OF UPPSALA, SWEDEN.

REFERENCES.

[1] L. Carlson, "On bounded analytic functions and closure problems," *Arkiv för Matematik*, vol. (1952), pp. 283-291.

[2] P. R. Garabedian, "Schwarz's lemma and the Szegö kernel function," *Transactions of the American Mathematical Society*, vol. 67 (1949), pp. 1-35.

[3] G. H. Hardy, J. E. Littlewood, G. Pólya, *Inequalities*, Cambridge, 1934.

[4] R. Nevanlinna, "Über beschränkte Funktionen die in gegebenen Punkten vorgeschriebene Werte annehmen," *Annales Academie Scientiarum Fennicae*, vol. 13 (1919), No. 1.

CONTINUITY OF SOLUTIONS OF PARABOLIC AND ELLIPTIC EQUATIONS.*

By J. NASH.

Introduction. Successful treatment of non-linear partial differential equations generally depends on "a priori" estimates controlling the behavior of solutions. These estimates are themselves theorems about linear equations with variable coefficients, and they can give a certain compactness to the class of possible solutions. Some such compactness is necessary for iterative or fixed-point techniques, such as the Schauder-Leray methods. Alternatively, the a priori estimates may establish continuity or smoothness of generalized solutions. The strongest estimates give quantitative information on the continuity of solutions without making quantitative assumptions about the continuity of the coefficients.

The theory of non-linear elliptic equations in two independent variables is fairly well developed. (See [1] for a survey and bibliography.) An essential part is the a priori Hölder continuity estimate for solutions of uniformly elliptic equations, first proved by Morrey in 1938. All methods used to obtain this estimate have been quite special to two dimensions, utilizing, for example, complex analysis and quasi-conformal mappings (see [2]). The restriction to two variables has been due to this use of such special methods; except for the crucial a priori estimate, the theory is extensible (and in large part has been extended) to n dimensions and to parabolic equations. Our results fill this gap, and it should now be possible to build a general theory of non-linear parabolic and elliptic equations, free of dimension restrictions. Strictly speaking, our work needs some generalization to cover equations with lower order terms, systems, etc. This generalization can probably be accomplished fairly quickly.

In this paper, we consider linear parabolic equations of the form

$$\sum_{i,j} \partial[C_{ij}(x_1, x_2, \cdots, x_n, t)\,\partial T/\partial x_j]/\partial x_i = \partial T/\partial t, \text{ or} \tag{1}$$
$$\nabla \cdot (C(x,t) \cdot \nabla T) = T_t,$$

---

* Received May 26, 1958.

where the C_{ij} form a symmetric real matrix $C(x,t)$ for each point x and time t. We assume there are universal bounds $c_2 \geqq c_1 > 0$ on the eigenvalues of C so that any eigenvalue θ_ν satisfies $c_1 \leqq \theta_\nu \leqq c_2$. This is the standard "uniform ellipticity" assumption. The continuity estimate for a solution $T(x,t)$ of (1) satisfying $|T| \leqq B$ and defined for $t \geqq t_0$ is

$$(2) \quad |T(x_1,t_1) - T(x_2,t_2)| \leqq BA\{[|x_1 - x_2|/(t_1 - t_0)^{\frac{1}{2}}]^{\alpha} + [(t_2 - t_1)/(t_1 - t_0)]^{\frac{1}{2}\alpha/(1+\alpha)}\},$$

where $t_2 \geqq t_1 > t_0$. Here A and α are a priori constants which depend only on c_1 and c_2 and the space dimension n. As a corollary of our results on parabolic equations, we obtain a continuity estimate for solutions of elliptic equations. If $T(x)$ satisfies $\nabla \cdot (C(x) \cdot \nabla T) = 0$ in a region R and the same bounds c_1 and c_2 limit the eigenvalues of $C(x)$, then

$$(3) \qquad |T(x_1) - T(x_2)| \leqq BA'(|x_1 - x_2|/d(x_1,x_2))^{\alpha/(1+\alpha)},$$

where α is the α of (2) and A' is an a priori constant $A'(n,c_1,c_2)$, and where $|T| \leqq B$ in R and $d(x_1,x_2)$ is the lesser of the distances of the points x_1 and x_2 from the boundary of R.

Our paper is arranged in six parts, each concluding with the attainment of a result significant in itself. Detailed proofs are given and all the results presented in [14] are covered. An appendix states further results, including continuity at the boundary in the Dirichlet problem, a Harnack inequality, and other results, stated without detailed proofs.

General remarks. The open problems in the area of non-linear partial differential equations are very relevant to applied mathematics and science as a whole, perhaps more so than the open problems in any other area of mathematics, and this field seems poised for rapid development. It seems clear, however, that fresh methods must be employed. We hope this paper contributes significantly in this way and also that the new methods used in our previous paper, reference [10], will be of value.

Little is known about the existence, uniqueness and smoothness of solutions of the general equations of flow for a viscous, compressible, and heat conducting fluid. These are a non-linear parabolic system of equations. Also the relationship between this continuum description of a fluid (gas) and the more physically valid statistical mechanical description is not well understood. (See [11], [12], and [13]). An interest in these questions led us to undertake this work. It became clear that nothing could be done about the continuum description of general fluid flow without the ability to handle non-linear parabolic equations and that this in turn required an a priori estimate of continuity, such as (2).

Probably one should first try to prove a conditional existence and uniqueness theorem for the flow equations. This should give existence, smoothness, and unique continuation (in time) of flows, conditional on the non-appearance of certain *gross* types of singularity, such as infinities of temperature or density. (A gross singularity could arise, for example, from a converging spherical shock wave.) A result of this kind would clarify the turbulence problem.

The methods used here were inspired by physical intuition, but the ritual of mathematical exposition tends to hide this natural basis. For parabolic equations, diffusion, Brownian movement, and flow of heat or electrical charges all provide helpful interpretations. Moreover, to us, parabolic equations seem more natural than elliptic ones. It is certainly true in principle that the theory of parabolic equations includes elliptic equations as a specialization, and in applications an elliptic equation typically arises as the description of the steady state of a system which in general is described by a parabolic equation.

In our work, no difference at all appears between dimensions two and three. Only in one dimension would the situation simplify. The key result seems to be the moment bound (13); it opens the door to the other results. We had to work hard to get (13), then the rest followed quickly.

We are indebted to several persons and institutions in connection with this work, including Bers, Beurling, Browder, Carleson, Lax, Levinson, Morrey, Newman, Nirenberg, Stein and Wiener, the Alfred P. Sloan Foundation, the Institute for Advanced Study, M. I. T., N. Y. U., and the Office of Naval Research.

Part I: The Moment Bound.

More than enough is known about linear parabolic equations with variable coefficients to assure the existence of well behaved solutions for equations of the form (1) if we make strong (qualitative) restrictions on the C_{ij} and restrict the class of solutions to be considered. (See [3] through [7].) Therefore we assume: (a) The $C_{ij}(x,t)$ are uniformly C^∞, (b) $C_{ij}(x,t) = \sqrt{c_1c_2}\,\delta_{ij}$ (Kronecker delta) for $|x| \geqq r_0$, some large constant. We consider only solutions $T(x,t)$ bounded in x for each t for which the solution is defined, i.e., $\max\limits_x |T(x,t)|$ is finite.

Under these restrictions, any bounded measurable function $T(x, t_0)$ of x given at an initial time t_0 determines a unique continuation $T(x, t)$ defined for all $t \geqq t_0$ and C^∞ for $t > t_0$. Moreover, $T(x, t) \to T(x, t_0)$ almost everywhere as $t \to t_0$, and $\max_x |T(x, t)|$ is non-increasing in t. It is also known that fundamental solutions, which we discuss below, exist and have the general properties we state. (See [4], [7].)

After the a priori results are established, a passage to the limit can remove the restrictions on the C_{ij}. This is a standard device in the use of a priori estimates. The Hölder continuity (2) makes the family of solutions equicontinuous and forces a continuous limit (generalized) solution to exist. Furthermore, the maximum principle remains valid and with it the unique continuability of solutions bounded in space. The final result requires only measurability for the C_{ij}, plus the uniform ellipticity condition; and the a priori estimates then hold for the generalized solutions.

The use of fundamental solutions is very helpful with equations of the form (1). Our work is built around step by step control of the properties of fundamental solutions and most of the results concern them directly. A fundamental solution $T(x, t)$ has a "source point" x_0 and "starting time" t_0 and is defined and positive for $t > t_0$. Also, $\int T(x, t)\, dx = 1$ for every $t > t_0$, where dx is the volume element in n-space. As $t \to t_0$, the fundamental solution concentrates around its source point; $\lim T(x, t)$ is zero unless $x = x_0$, in which case it is $+\infty$. Physically, a fundamental solution represents the concentration of a diffusant spreading from an initial concentration of unit weight at x_0 at time t_0.

All fundamental solutions are conveniently unified in a "characterizing function" $S(x, t, \bar{x}, \bar{t})$. For fixed $\bar{x}$ and $\bar{t}$ and as a function of x and t, S is a fundamental solution of (1) with source point $\bar{x}$ and starting time $\bar{t}$. Dually, for fixed x and t, S is a fundamental solution of the adjoint equation: $\nabla_{\bar{x}} \cdot [C(\bar{x}, t) \cdot \nabla_{\bar{x}} S] = -\partial S / \partial \bar{t}$, where time runs backwards. This duality enables us to use estimates for fundamental solutions in two ways on S.

The dependence of a bounded solution $T(x, t)$ on bounded initial data $T(x, t_0)$ is expressible through S:

$$T(x, t) = \int S(x, t, \bar{x}, t_0) T(\bar{x}, t_0)\, d\bar{x}; \tag{4}$$

in particular,

$$S(x_2, t_2, x_0, t_0) = \int S(x_2, t_2, x_1, t_1) S(x_1, t_1, x_0, t_0)\, dx_1. \tag{5}$$

These are standard relations. (5) reveals a reproductive property of fundamental solutions.

Now consider a special fundamental solution $T = T(x,t) = S(x,t,0,0)$ with source at the origin and starting time zero. Let

$$E = \int T^2\, dx,$$

then

$$E_t = 2\int T T_t\, dx = 2\int T \nabla \cdot (C \cdot \nabla T)\, dx = -2\int \nabla T \cdot C \cdot \nabla T\, dx,$$

by integration by parts. For any vector V, we have $c_1 | V |^2 \leqq V \cdot C \cdot V \leqq c_2 | V |^2$; therefore

$$-E_t \geqq 2c_1 \int | \nabla T |^2\, dx. \tag{6}$$

With (6) and a lower bound for $\int | \nabla T |^2\, dx$ in terms of E, we shall be able to bound E above, obtaining our first a priori estimate. To bound $\int | \nabla T |^2\, dx$ we employ a general inequality valid for any function $u(x)$ in n-space. For our purposes, we assume u is smooth and well behaved at infinity. E. M. Stein gave us the quick proof which follows below.

The Fourier transform of $u(x)$ is

$$v(y) = (2\pi)^{-n/2} \int e^{ix\cdot y} u(x)\, dx.$$

This has the familiar property

$$\int | v |^2 dy = \int | u |^2 dx.$$

The transform of $\partial u/\partial x_k$ is $iy_k v$; hence

$$\int | \partial u/\partial x_k |^2\, dx = \int y_k^2 \, | v |^2\, dy,$$

and

$$\int | \nabla u |^2\, dx = \sum_i \int (\partial u/\partial x_k)^2\, dx = \int | y |^2 | v |^2\, dy.$$

Finally,

$$| v | \leqq (2\pi)^{-n/2} \int | e^{ix\cdot y} | \cdot | u |\, dx = (2\pi)^{-n/2} \int | u |\, dx;$$

therefore, for any $\rho > 0$, we have

$$\int_{|y| \leqq \rho} | v |^2\, dy \leqq (\pi^{n/2}\rho^n/(n/2)\,!) \{ (2\pi)^{-n/2} \int | u |\, dx \}^2, \tag{a}$$

using the formula for the volume of an n-sphere. On the other hand,

$$\int_{|y|>\rho} | v |^2\, dy \leqq \int_{|y|>\rho} | y/\rho |^2 \, | v |^2\, dy = \rho^{-2} \int | \nabla u |^2\, dx. \tag{b}$$

If we choose the value of ρ minimizing the sum of the two bounds (a) and (b), we obtain a bound on $\int | v |^2\, dy = \int | u |^2\, dx$ in terms of $\int | u |\, dx$ and $\int | \nabla u |^2\, dx$. Solved for $\int | \nabla u |^2\, dx$, this is

$$\int |\nabla u|^2\, dx$$
$$\geqq (4\pi n/(n+2))\,[(n/2)\,!/(1+n/2)]^{2/n}\,[\int |u|\, dx]^{-4/n}\,[\int |u|^2\, dx]^{1+2/n}.$$

Applying the above inequality with $u = T$, remembering that $\int T dx = 1$, we obtain from (6)

$$-E_t \geqq kE^{1+2/n}.$$

This is the first use of a convention we now establish that k is a generic symbol for a priori constants which depend only on n, c_1, and c_2. Any two instances of k should be presumed to be different constants. Thus, from the above inequality, $(E^{-2/n})_t \geqq k$; hence $E^{-2/n} \geqq kt$ and

$$E \leqq kt^{-n/2}. \tag{7}$$

We used above the qualitative fact $\lim\limits_{t\to 0} E = \infty$.

From this first bound (7) and the identity (5), we obtain

$$T(x,t) = \int S(x,t,\bar{x},t/2)\,S(\bar{x},t/2,0,0)\,d\bar{x},$$

whence

$$(T(x,t))^2 \leqq \int [S(x,t,\bar{x},t/2)]^2\, d\bar{x} \cdot \int [S(\bar{x},t/2,0,0)]^2\, d\bar{x} \leqq [k(t/2)^{-n/2}]^2.$$

Therefore

$$T \leqq kt^{-n/2}, \tag{8}$$

which is a pointwise bound, stronger than (7).

The key estimate controls the "moment" of a fundamental solution

$$M = \int rT\, dx = \int |x|\, T\, dx.$$

To prove $M \leqq kt^{\frac{1}{2}}$ is our first major goal. This is dimensionally the only possible form for a bound on M. The moment bound is essential to all subsequent parts of this paper.

We also define an "entropy."

$$Q = -\int T \log T\, dx. \tag{9}$$

From (8),

$$Q \geqq \int \min_x [-\log T]\,(T\, dx) \geqq -\log(kt^{-n/2}) \int T\, dx,$$

hence

$$Q \geqq \pm k + \tfrac{1}{2} n \log t \tag{10}$$

because $\int T\, dx = 1$. The sharp result $Q \geqq \frac{1}{2} n \log(4\pi e c_1 t)$ is obtainable from a more sophisticated argument.

Our derivation of a bound on M requires a lower bound on M in terms of Q as a lemma. This inequality, which is $M \geqq ke^{Q/n}$, depends only on the facts $T \geqq 0$, $\int T\,dx = 1$. First observe that for any fixed λ,

$$\min_T (T \log T + \lambda T) = -e^{-\lambda-1}.$$

Let $\lambda = ar + b$, where $r = |x|$ and a and b are any constants, and integrate over space, obtaining

$$\int [T \log T + (ar + b)T]\,dx \geqq -e^{-b-1} \int e^{-ar}\,dx,$$

or

$$-Q + aM + b \geqq -e^{-b-1} a^{-n} D_n,$$

where D_n is the well known constant $2^n \pi^{\frac{1}{2}(n-1)} [\frac{1}{2}(n-1)]!$ related to the gamma-function and the surface of the $(n-1)$-sphere. Now set $a = n/M$ and $e^{-b} = (e/D_n) \cdot a^n$. Then $-Q + n + b \geqq -1$ or $n + 1 \geqq Q + \log(n/D_n) + \log(n/M)$; thus $n \log M + n \geqq Q + n \log n - \log D_n$, finally,

$$M \geqq (n/e\, D_n{}^{1/n}) e^{Q/n} = ke^{Q/n}. \tag{11}$$

This ingenious proof, due to L. Carleson, gives an optimal constant.

The next inequality is a "dynamic" one, connecting the rates of change with time of M and Q. Differentiating (9),

$$\begin{aligned} Q_t = -\int (1 + \log T) T_t\,dx &= -\int (1 + \log T) \nabla \cdot (C \cdot \nabla T)\,dx \\ &= \int \nabla (\log T) \cdot C \cdot \nabla T\,dx \end{aligned}$$

after integration by parts. This can be rewritten

$$Q_t = \int \nabla (\log T) \cdot C \cdot \nabla (\log T)\,(T\,dx).$$

Since in general $V \cdot c_2 C \cdot V \geqq V \cdot C^2 \cdot V = |C \cdot V|^2$, where V is a vector, we have

$$\begin{aligned} c_2 Q_t \geqq \int |C \cdot \nabla (\log T)|^2 (T\,dx) &\geqq [\int |C \cdot \nabla \log T|\,(T\,dx)]^2 \\ &\geqq [\int |C \cdot \nabla T|\,dx]^2. \end{aligned}$$

Here we used the Schwarz inequality in the form $\int_0^1 f^2\,du \geqq [\int_0^1 f\,du]^2$ with du corresponding to $T\,dx$.

By analogous manipulations,

$$M_t = -\int \nabla r \cdot C \cdot \nabla T\,dx \quad\text{and}\quad |M_t| \leqq \int |\nabla r|\,|C \cdot \nabla T|\,dx,$$

hence,

$$|M_t| \leqq \int |C \cdot \nabla T|\,dx.$$

Combining inequalities,

$$c_2 Q_t \geqq (M_t)^2. \tag{12}$$

This is a powerful inequality. Q is defined as it is in order to obtain (12).

The three inequalities

$$Q \geqq \pm k + \tfrac{1}{2} n \log t \tag{10}$$

$$M \geqq k e^{Q/n} \tag{11}$$

$$c_2 Q_t \geqq (M_t)^2 \tag{12}$$

and the qualitative fact $\lim M = 0$, as $t \to 0$, suffice by themselves to bound above and below both M and Q, as functions of time. No further reference to the differential equation is needed.

From $M(0) = 0$ and (12),

$$M \leqq \int_0^t (c_2 Q_t)^{\frac{1}{2}}\, dt,$$

whence

$$k e^{Q/n} \leqq M \leqq \int_0^t (c_2 Q_t)^{\frac{1}{2}}\, dt.$$

Now define $nR = Q \mp k - \frac{1}{2} n \log t$ in such a way that $R \geqq 0$ corresponds to (10). Then $Q_t = nR_t + n/2t$, and we obtain

$$k t^{\frac{1}{2}} e^R \leqq M \leqq (nc_2)^{\frac{1}{2}} \int_0^t (1/2t + R_t)^{\frac{1}{2}}\, dt.$$

When a and $a+b$ are positive $(a+b)^{\frac{1}{2}} \leqq a^{\frac{1}{2}} + b/2a^{\frac{1}{2}}$, hence

$$\int_0^t (1/2t + R_t)^{\frac{1}{2}}\, dt \leqq \int_0^t (1/2t)^{\frac{1}{2}} dt + \int_0^t (t/2)^{\frac{1}{2}} R_t\, dt$$

$$\leqq (2t)^{\frac{1}{2}} + R(t/2)^{\frac{1}{2}} - \int_0^t R/(8t)^{\frac{1}{2}} dt \leqq (2t)^{\frac{1}{2}} + R(t/2)^{\frac{1}{2}}.$$

Here we used integration by parts and $R \geqq 0$ in the second and third steps. Applying this result,

$$k t^{\frac{1}{2}} e^R \leqq kM \leqq (2t)^{\frac{1}{2}} + R(t/2)^{\frac{1}{2}},$$

or

$$k e^R \leqq kM/t^{\frac{1}{2}} \leqq 2^{\frac{1}{2}}(1 + \tfrac{1}{2} R).$$

Clearly ke^R increases faster in R than $2^{\frac{1}{2}}(1 + \frac{1}{2} R)$ so that R must be bounded above. Therefore $M/t^{\frac{1}{2}}$ is bounded both above and below:

$$k t^{\frac{1}{2}} \leqq M \leqq k t^{\frac{1}{2}}. \tag{13}$$

If we use best possible constants in (10) and (11), we can obtain

$$b_n(2c_1nt)^{\frac12} \leqq M \leqq (2c_2nt)^{\frac12}[1+\min(\lambda, (\lambda/2)^{\frac12})],$$

where

$$b_n = (n/2t)^{\frac12}\{\pi^{\frac12}/[\tfrac12(n-1)]\,!\}^{1/n} \geqq 2^{-1/2n}$$

and

$$\lambda = \tfrac12\log(c_2/c_1) - \log b_n \leqq (1/2n)\log 2 + \tfrac12\log(c_2/c_1).$$

Thus λ is relatively small. Since $b_n \rightarrow 1$ as $n \rightarrow \infty$, the bounds sharpen with increasing n; indeed, they seem surprisingly sharp. For comparison, $M = (2nct)^{\frac12}$ in the simple heat equation where $C_{ij} = c\delta_{ij}$ and $c_1 = c_2 = c$.

Part II: The *G* Bound.

Here we obtain a result limiting the extent to which a fundamental solution can be very small over a large volume of space near its source point. From this result, we can show there is some overlap, defined as $\int \min(T_1, T_2)dx$, of two fundamental solutions with nearby source points, starting simultaneously.

Let T be $S(x, t, 0, 0)$ and let

$$U(\xi, t) = t^{n/2}T(t^{\frac12}\xi, t). \tag{14}$$

This coordinate transformation and renormalization makes $\int U\, d\xi = 1$, where $d\xi$ is the volume element. Furthermore, if μ is the constant such that $M \leqq \mu t^{\frac12}$, we have $\int |\xi|U\, d\xi \leqq \mu$. For U, equation (1) transforms to

$$2tU_t = nU + \xi\cdot\nabla U + 2\nabla\cdot(C\cdot\nabla U). \tag{15}$$

Let

$$G = \int \exp(-|\xi|^2)\log(U + \delta)\, d\xi, \tag{16}$$

where δ is a small positive constant. G is sensitive to areas where $|\xi|$ is not large and U is small. These tend to make G strongly negative. We later obtain a lower bound on G of the form

$$G \geqq -k(-\log\delta)^{\frac12},$$

valid for sufficiently small δ. This bound limits the possibility for U to be small in a large portion of the region where $|\xi|$ is not large. From $U > 0$ the weak lower bound $G > \pi^{n/2}\log\delta$ follows immediately.

Differentiating (16) with respect to time and using (15), we obtain

$$2tG_t = H_1 + H_2 + H_3,$$

where

$$H_1 = n\int \exp(-|\xi|^2)U/(U+\delta)\,d\xi \geqq 0,$$

$$H_2 = \int \exp(-|\xi|^2)\xi\cdot\nabla\log(U+\delta)\,d\xi$$
$$= -\int \nabla\cdot[\exp(-|\xi|^2)\xi]\log(U+\delta)\,d\xi,$$

by integration by parts, so that

$$H_2 = -\int \exp(-|\xi|^2)(\nabla\cdot\xi)\log(U+\delta)\,d\xi$$
$$+\int \exp(-|\xi|^2)(2|\xi|\nabla|\xi|)\cdot\xi\log(U+\delta)\,d\xi$$
$$= -nG + 2\int \exp(-|\xi|^2)|\xi|^2[\log\delta + \log(1+U/\delta)]\,d\xi,$$

hence,

$$H_2 \geqq -nG + 2\log\delta\int|\xi|^2\exp(-|\xi|^2)\,d\xi \geqq -nG + n\pi^{n/2}\log\delta;$$

finally

$$H_3 = 2\int \exp(-|\xi|^2)\nabla\cdot(C\cdot\nabla U)/(U+\delta)\,d\xi$$
$$= -2\int \nabla[\exp(-|\xi|^2)/(U+\delta)]\cdot C\cdot\nabla U\,d\xi$$
$$= 4\int (\exp(-|\xi|^2)[|\xi|\nabla|\xi|\cdot C\cdot\nabla U]/(U+\delta)\,d\xi$$
$$+ 2\int \exp(-|\xi|^2)[\nabla U\cdot C\cdot\nabla U]/(U+\delta)^2\,d\xi$$
$$= H_3' + H_3'',$$

where

$$H_3' = 4\int \exp(-|\xi|^2)\xi\cdot C\cdot\nabla\log(U+\delta)\,d\xi,$$
$$H_3'' = 2\int \exp(-|\xi|^2)\nabla\log(U+\delta)\cdot C\cdot\nabla\log(U+\delta)\,d\xi.$$

From the Schwarz inequality,

$$(H_3')^2 \leqq \{4\int \exp(-|\xi|^2)\xi\cdot C\cdot\xi\,d\xi\}$$
$$\times\{4\int \exp(-|\xi|^2)\nabla\log(U+\delta)\cdot C\cdot\nabla\log(U+\delta)\,d\xi\}$$
$$\leqq \{4c_2\int|\xi|^2\exp(-|\xi|^2)\,d\xi\}2H_3''$$
$$\leqq (4c_2\cdot\tfrac{1}{2}n\pi^{\frac{1}{2}n})\cdot 2H_3'' = 4nc_2\pi^{\frac{1}{2}n}H_3''.$$

Hence

$$|H_3'| \leqq k(H_3'')^{\frac{1}{2}}.$$

Furthermore,

$$H_3'' \geqq 2c_1\int \exp(-|\xi|^2)|\nabla\log(U+\delta)|^2\,d\xi \tag{17}$$

Combining the lower bounds available for H_1, H_2, and H_3', we obtain

$$(18)\qquad \begin{aligned} 2tG_t &\geqq H_1 + H_2 + H_3'' - |H_3'| \\ &\geqq 0 + (-nG + n\pi^{\frac{1}{2}n}\log\delta) + H_3'' - k(H_3'')^{\frac{1}{2}} \\ &\geqq k\log\delta - nG - k(H_3'')^{\frac{1}{2}} + H_3''. \end{aligned}$$

When we bound H_3'' below in terms of G, (18) will yield a lower bound on G.

A function $f(\xi) = f(\xi_1, \xi_2, \cdots, \xi_n)$ may be expanded in products of Hermite polynomials, of the form $\prod H_{\nu(i)}(\xi_i)$, where the polynomials are defined and orthonormalized so that $\int_{-\infty}^{+\infty} \exp(-s^2) H_\nu(s) H_\lambda(s)\, ds = \delta_{\nu\lambda}$. The identity $dH_\nu(s)/ds = (2\nu)^{\frac{1}{2}} H_{\nu-1}(s)$ obtains, and the coefficients of these products in the similar expansion of, say, $\partial f/\partial \xi_i$ depend very simply on the coefficients in the expansion of f. If $\int \exp(-|\xi|^2) f\, d\xi = 0$, the coefficient of $\prod H_0(\xi_i)$ is zero and we obtain

$$\int \exp(-|\xi|^2) |\nabla f|^2\, d\xi = \sum \int \exp(-|\xi|^2)(\partial f/\partial \xi_i)^2 d\xi \geqq 2\int \exp(-|\xi|^2) f^2\, d\xi.$$

Applying the above, with $f = \log(U + \delta) - \pi^{-n/2} G$, to (17), we obtain

$$(19)\qquad H_3'' \geqq 4c_1 \int \exp(-|\xi|^2)[\log(U+\delta) - \pi^{-n/2}G]^2\, d\xi.$$

The quantity $U^{-1}[\log(U+\delta) - \pi^{-n/2}G]^2$, related to the integrand in (19), is large for very small U, then decreases to zero, rises from zero to a local maximum at $U = U_c$, say, and finally decreases monotonically as $U \to \infty$ for $U \geqq U_c$. (We know $\log\delta - \pi^{-n/2}G < 0$.) The equation for the maximum point U_c is $\log(U_c + \delta) - \pi^{-n/2}G = 2U_c/(U_c + \delta)$, from which $U_c < U_0 = \exp(2 + \pi^{-n/2}G)$. Therefore the quantity under discussion is decreasing for $U \geqq U_0$ The bound (8), $T \leqq kt^{-n/2}$, corresponds to $U \leqq k$. Hence the quantity has a lower bound of the form $k[\log(k+\delta) - kG]^2$ for $U \geqq U_0$. Applying this to (19), we may say

$$H_3'' \geqq 4c_1 \int \exp(-|\xi|^2) k[\log(k+\delta) - kG]^2 U^*\, d\xi,$$

where $U^* = U$ for $U > U_0$ and $U^* = 0$ for $U \leqq U_0$. Thus we are ignoring the contribution to (19) of the region where $U \leqq U_0$ and taking the worst case, U as large as possible, in the remaining region. For sufficiently negative G, the expression $\log(k+\delta) - kG$ will remain positive when δ is omitted, so that $[\log k - kG]^2 < [\log(k+\delta) - kG]^2$, and we can simplify the above inequality on H_3'' to the form

$$(20)\qquad H_3'' \geqq (k - kG)^2 \int \exp(-|\xi|^2) U^*\, d\xi.$$

Let $\lambda = \int U^*\, d\xi$ and observe that $\int |\xi|\, U^*\, d\xi \leqq \int |\xi|\, U\, d\xi \leqq \mu$. Therefore

$$\mu \geqq \int_{|\xi| \geqq 2\mu/\lambda} |\xi| U^* \, d\xi \geqq (2\mu/\lambda) \int_{|\xi| \geqq 2\mu/\lambda} U^* \, d\xi,$$

hence,

$$\int_{|\xi| \geqq 2\mu/\lambda} U^* \, d\xi \leqq \tfrac{1}{2}\lambda, \text{ and so } \int_{|\xi| \leqq 2\mu/\lambda} U^* \, d\xi \geqq \lambda - \tfrac{1}{2}\lambda = \tfrac{1}{2}\lambda.$$

This result can be applied to (20) and yields

$$H_3'' \geqq (k - kG)^2 \cdot \exp(-(2\mu/\lambda)^2)(\tfrac{1}{2}\lambda). \tag{21}$$

This is not effective unless we can bound λ below, or bound $\int \hat{U} \, d\xi = 1 - \lambda$ above, where $\hat{U} = U - U^*$ so that $\hat{U} = 0$ unless $U \leqq U_0$, in which case $\hat{U} = U$. Of course, we know $\int |\xi| \hat{U} \, d\xi \leqq \mu$ because $\hat{U} \leqq U$. Under the moment constraint and the constraint $\hat{U} \leqq U_0$, the maximum of $\int \hat{U} \, d\xi$ is clearly realized by having $\hat{U} = U_0$ for $|\xi| \leqq \rho$ and $\hat{U} = 0$ for $|\xi| > \rho$, where ρ is such that

$$\int |\xi| \hat{U} \, d\xi = \int |\xi| U_0 \, d\xi = [n\pi^{n/2}/(n+1)(n/2)!]\rho^{n+1} U_0 = \mu.$$

This makes

$$1 - \lambda = \int \hat{U} \, d\xi = [\pi^{n/2}/(n/2)!]\rho^n U_0,$$

$$1 - \lambda \leqq U_0 (k\mu/U_0)^{n/(n+1)} \text{ or } 1 - \lambda \leqq k U_0^{1/(n+1)}.$$

If U_0, which is $\exp(2 + \pi^{-n/2} G)$, is small enough, then $1 - \lambda$ is small and λ is bounded below. Thus $\lambda \geqq \frac{1}{2}$, say, for all sufficiently large $-G$. Now from (21), we have

$$H_3'' \geqq (k - kG)^2$$

for sufficiently large $-G$.

Returning to inequality (18) controlling G_t and applying the above result, we can state that *for sufficiently negative* G,

$$\begin{aligned} 2dG/d(\log t) = 2tG_t &\geqq -nG + k \log \delta + (k - kG)^2 - k(k - kG) \\ &\geqq k\,|G|^2 + k \log \delta. \end{aligned} \tag{22}$$

Let $G_1(c_1, c_2, n)$ be the number such that when $G \leqq G_1$, we know G is small enough to make (22) valid. Let $G_2(c_1, c_2, n, \delta) = -k(-\log \delta)^{\frac{1}{2}}$ be the largest number such that $k\,|G|^2 + k \log \delta > 0$ for all $G < G_2$. Then $\min(G_1, G_2) = G_3$ is the smallest possible value of G. If we had $G(t_1) = G_3 - \epsilon$, we would have $dG/d(\log t) \geqq \epsilon^*$ for all $t \leqq t_1$, and consequently $G(t) \leqq G(t_1) - \epsilon^* \log(t_1/t)$, which implies $G \to -\infty$ as $t \to 0$. But since $G \geqq \pi^{n/2} \log \delta$, the hypothesis $G(t_1) = G_3 - \epsilon$ is impossible. Our conclusion is $G \geqq G_3$, or

$$G \geqq -k(-\log \delta)^{\frac{1}{2}} \tag{23}$$

for all *sufficiently small values of* δ, because $G_2 \leqq G_1$ and

$$G_3 = G_2 = -k(-\log\delta)^{\frac{1}{2}}$$

when δ is small enough.

Part III: The Overlap Estimate

Let T_1 and T_2 be two fundamental solutions $S(x,t,x_1,0)$ and $S(x,t,x_2,0)$ with nearby sources. Change coordinates, defining $U_1 = t^{n/2}T_1(t^{\frac{1}{2}}\xi, t)$ and $U_2 = t^{n/2}T_2(t^{\frac{1}{2}}\xi, t)$. Let $\xi_1 = x_1/t^{\frac{1}{2}}$ and $\xi_2 = x_2/t^{\frac{1}{2}}$. Here the source of the (renormalized) fundamental solution U_i is ξ_i rather than the origin, which was the source of U in Part II. Taking this into account, we apply (23), obtaining

$$\int \exp(-|\xi - \xi_i|^2)\log(U_i + \delta)\,d\xi = G_i \geqq -k(-\log\delta)^{\frac{1}{2}},$$

where $i = 1$ or 2 and δ must be sufficiently small. We may add the inequalities above and obtain

$$\int \max_i[\exp(-|\xi - \xi_i|^2)]\max_i[\log(U_i + \delta)]\,d\xi \\ + \int \min_i[\exp(-|\xi - \xi_i|^2)]\min_i[\log(U_i + \delta)]\,d\xi \geqq -2k(-\log\delta)^{\frac{1}{2}}$$

in which we form two integrals with sum at least as large as the sum of the original integrals. We abbreviate the above to

$$\int f^* \log(U_{\max} + \delta)\,d\xi + \int \hat{f}\log(U_{\min} + \delta)\,d\xi \geqq -k(-\log\delta)^{\frac{1}{2}}.$$

For the first integral, we observe (assuming $\delta \leqq 1$)

$$\int f^* \log(U_{\max} + \delta)\,d\xi \leqq \int f^*(U_1 + U_2)\,d\xi \leqq \int (U_1 + U_2)\,d\xi = 2.$$

For the second integral,

$$\int \hat{f}\log(U_{\min} + \delta)\,d\xi \leqq \log\delta \int \hat{f}\,d\xi + \max[\hat{f}]\int \log(1 + U_{\min}/\delta)\,d\xi \\ \leqq w\log\delta + \delta^{-1}\int U_{\min}\,d\xi,$$

where

$$w = \int \min[\exp(-|\xi - \xi_1|^2), \exp(-|\xi - \xi_2|^2)]\,d\xi.$$

Therefore we obtain

$$2 + w\log\delta + \delta^{-1}\int \min(U_1, U_2)\,d\xi \geqq -k(-\log\delta)^{\frac{1}{2}},$$

or

$$\text{(24)} \quad \int \min(T_1, T_2)\,dx = \int \min(U_1, U_2)\,d\xi \geqq \delta[-2 - w\log\delta - k(-\log\delta)^{\frac{1}{2}}].$$

This is valid for sufficiently small δ, say for $\delta \leqq \delta_1$. Also, there is a value $\delta_2(w)$ such that for $\delta < \delta_2(w)$, the bracketed expression is positive. If we set $\delta = \frac{1}{2}\min(\delta_1, \delta_2)$, the right member of (24) is definitely positive, and we may conclude

$$(25) \qquad \int \min(T_1, T_2)\,dx \geqq \phi(|\xi_1 - \xi_2|) \geqq \phi(|x_1 - x_2|/t^{\frac{1}{2}})$$

because w is a function of $|\xi_1 - \xi_2|$. The function ϕ is decreasing but always positive. It is an a priori function, determined only by c_1, c_2, and n. This inequality (25) is our first estimate on the overlap of fundamental solutions. Its weakness is that we know little about the function ϕ.

Part IV: Continuity in Space.

We can obtain a stronger inequality by iterative use of (25). Observe that

$$(26) \qquad \tfrac{1}{2}\int |T_1 - T_2|\,dx = \tfrac{1}{2}\int [T_1 + T_2 - 2\min(T_1, T_2)]\,dx$$
$$\leqq 1 - \phi(|x_1 - x_2|/t^{\frac{1}{2}}) = \psi(|x_1 - x_2|/t^{\frac{1}{2}})$$

in which we define the function ψ, which is increasing but always less than one.

Let $T_a = \max(T_1 - T_2, 0)$ and $T_b = \max(T_2 - T_1, 0)$ so that $T_a + T_b = |T_1 - T_2|$ and $\int (T_a - T_b)\,dx = \int (T_1 - T_2)\,dx = 0$. Then

$$\int T_a dx = \int T_b dx = A(t) = \tfrac{1}{2}\int |T_1 - T_2|\,dx \leqq \psi(|x_1 - x_2|/t^{\frac{1}{2}}),$$

defining $A(t)$. Let

$$\chi(x, \bar{x}, t) = T_a(x)T_b(\bar{x})/A(t).$$

Let $T_a{}^*(x', t', t)$ be the bounded solution in x' and t' of (1) defined for $t' \geqq t$ and having the initial value $T_a{}^*(x, t, t) = T_a(x, t)$. Define $T_b{}^*$ similarly. Then from (4),

$$T_a{}^*(x', t', t) = \int S(x', t', x, t)T_a(x, t)\,dx$$
$$= \int\int S(x', t', x, t)\chi(x, \bar{x}, t)\,dx\,d\bar{x},$$

and

$$T_1(x', t') - T_2(x', t') = T_a{}^* - T_b{}^*$$
$$= \int\int [(x', t', x, t) - S(x', t', \bar{x}, t)]\chi(x, \bar{x}, t)\,dx\,d\bar{x}$$

by the superposition principle ($T_1 - T_2$ and $T_a{}^* - T_b{}^*$ are both solutions of (1) for $t' \geqq t$, and by definition, $T_a{}^* - T_b{}^* = T_1 - T_2$ at $t' = t$.). Integrating this over dx', we obtain

$$\tfrac{1}{2}\int |T_1(x',t') - T_2(x',t')|\, dx'$$
$$\leqq \int\int\int |S(x',t',x,t) - S(x',t',\bar{x},t)|\, dx'\, \chi(x,\bar{x},t)\, dx\, d\bar{x},$$

whence

$$A(t') \leqq \int\int \psi(|x-\bar{x}|/(t'-t)^{\frac{1}{2}})\chi(x,\bar{x},t)\, dx\, d\bar{x} \tag{27}$$

by application of (26). Incidentally, the right member above is

$$\leqq \int\int \chi(x,\bar{x},t)\, dx\, d\bar{x} = A(t),$$

thus $A(t') \leqq A(t)$ when $t' \geqq t$. This inequality (27) is the key to the iterative argument which strengthens (25) and (26).

To begin the iterative argument, we choose any specific number d and let $\epsilon = \phi(d) = 1 - \psi(d)$. (If we were trying to get an explicit formula for the exponent α in (2), we would choose d with regard to an explicit formula for $\phi(d)$ so as to optimize the result.) Let $\sigma = 1 - \epsilon/4$. For each integer ν, let t_ν be the time (or the least time) at which $A(t) = A(t_\nu) = \sigma^\nu$, if t_ν exists. This is in reference to a specific pair, T_1 and T_2, of fundamental solutions. We know, for example, that $t_1 < \tau$, where $\tau = |x_1 - x_2|^2/d^2$, because $A(\tau) \leqq \psi(|x_1 - x_2|/\tau^{\frac{1}{2}}) = \psi(d) = 1 - \epsilon$ and $\sigma = 1 - \epsilon/4 > 1 - \epsilon$, so that $A(\tau) < A(t_1) = \sigma$.

Let $M_a(t) = \int |x - x_0|\, T_a dx$, where x_0 is $\frac{1}{2}(x_1 + x_2)$, the midpoint of the line segment joining the source points x_1 and x_2 of the fundamental solutions T_1 and T_2. Define M_b similarly and let $M_\nu = \max[M_a(t_\nu), M_b(t_\nu)]$. We decompose T_a into nearer and farther parts T_a' and $T_a - T_a'$ at each time t_ν as follows: for $|x - x_0| \leqq 2\sigma^{-\nu}M_\nu$, define $T_a' = T_a$; otherwise $T_a' = 0$. Then $2\sigma^{-\nu}M_\nu \int (T_a - T_a')\, dx \leqq \int |x - x_0|(T_a - T_a')\, dx \leqq \int |x - x_0|\, T_a dx \leqq M_\nu$, and consequently, $\int (T_a - T_a')dx \leqq \frac{1}{2}\sigma^\nu$ and $\int T_a'\, dx \geqq \frac{1}{2}\sigma^\nu$. Define T_b' similarly and define $\chi_\nu'(x,\bar{x}) = \sigma^{-\nu}T_a'(x)T_b'(\bar{x})$. Now, applying (27) with $t = t_\nu$, we can say

$$A(t') \leqq \int\int \psi(|x-\bar{x}|)/(t'-t_\nu)^{\frac{1}{2}}[\{\chi(x,\bar{x},t_\nu) - \chi_\nu'(x,\bar{x})\} + \chi_\nu'(x,\bar{x})]\, dx d\bar{x}$$
$$\leqq \int\int \{\chi - \chi_\nu'\} dx d\bar{x} + \psi(4\sigma^{-\nu}M_\nu/(t'-t_\nu)^{\frac{1}{2}}) \int\int \chi_\nu'\, dx d\bar{x},$$

because when $\chi_\nu' > 0$, we know both $T_a' > 0$ and $T_b' > 0$ so that both $|x - x_0|$ and $|\bar{x} - x_0|$ are $\leqq 2\sigma^{-\nu}M_\nu$, and consequently, $|x - \bar{x}| \leqq 4\sigma^{-\nu}M_\nu$, and we also know that $\chi \geqq \chi_\nu'$ and $\psi < 1$. Proceeding further,

$$A(t') \leqq \int\int \chi\, dx d\bar{x} - [1 - \psi(4\sigma^{-\nu}M_\nu/(t'-t_\nu)^{\frac{1}{2}})] \int\int \chi_\nu'\, dx d\bar{x}$$
$$\leqq \sigma^\nu - [1-\psi]\sigma^{-\nu} \int T_a' dx \int T_b' dx \leqq \sigma^\nu - [1-\psi]\sigma^{-\nu}(\sigma^\nu/2)^2$$
$$\leqq \sigma^\nu[3/4 + 1/4\psi(4\sigma^{-\nu}M_\nu/(t'-t_\nu)^{\frac{1}{2}})].$$

We now set $t' = t_\nu + 16\sigma^{-2\nu}(M_\nu)^2 d^{-2}$, and the argument of ψ above becomes d. Then since $\psi(d) = 1 - \epsilon$, we obtain

$$A(t') \leqq \sigma^\nu[3/4 + 1/4(1-\epsilon)] = \sigma^\nu(1-\epsilon/4) = \sigma^{\nu+1}.$$

Hence

$$t_{\nu+1} \leqq t' = t_\nu + 16\sigma^{-2\nu}(M_\nu)^2 d^{-2}. \tag{28}$$

This will bound the sequence $\{t_\nu\}$ of times after we obtain a bound on the sequence $\{M_\nu\}$ of moments.

Observe that

$$\begin{aligned} T_a(x',t') &= \max(T_1(x',t') - T_2(x',t'), 0) \\ &= \max(T_a^*(x',t',t) - T_b^*(x',t',t), 0) \leqq T_a^*(x',t',t) \\ &= \int S(x',t',x,t) T_a(x,t)\, dx. \end{aligned}$$

Therefore

$$\begin{aligned} M_a(t') &= \int | x' - x_0 | T_a(x',t')\, dx' \\ &\leqq \int\int [| x' - x | + | x - x_0 |] S(x',t',x,t) T_a(x,t)\, dx dx'; \end{aligned}$$

hence

$$\begin{aligned} M_a(t') \leqq &\int | x - x_0 | T_a(x,t) \int S(x',t',x,t)\, dx' dx \\ &+ \int T_a(x,t) \int | x' - x | S(x',t',x,t)\, dx' dx, \end{aligned}$$

or

$$\begin{aligned} M_a(t') &\leqq \int | x - x_0 | T_a(x,t)\, dx + \mu(t'-t)^{\frac{1}{2}} \int T_a(x,t)\, dx \\ &\leqq M_a(t) + A(t)\mu(t'-t)^{\frac{1}{2}}. \end{aligned}$$

Now let t and t' be t_ν and $t_{\nu+1}$, use a similar estimate for M_b and the definition $M_\nu = \max(M_a(t_\nu), M_b(t_\nu))$, and obtain, by (28),

$$\begin{aligned} M_{\nu+1} &\leqq M_\nu + \sigma^\nu \mu (t_{\nu+1} - t_\nu)^{\frac{1}{2}} \\ &\leqq M_\nu + \sigma^\nu \mu (16\sigma^{-2\nu}(M_\nu)^2 d^{-2})^{\frac{1}{2}} \leqq M_\nu(1 + 4\mu/d). \end{aligned}$$

Now $t_0 = 0$ and $M_0 = M_a(t_0) = M_b(t_0) = \frac{1}{2} | x_1 - x_2 |$, because T_1 and T_2 concentrate at x_1 and x_2 as $t \to 0$, and $| x_1 - x_0 | = | x_2 - x_0 | = \frac{1}{2} | x_1 - x_2 |$ since $x_0 = \frac{1}{2}(x_1 + x_2)$. Therefore we have

$$M_\nu \leqq \tfrac{1}{2} | x_1 - x_2 | (1 + 4\mu/d)^\nu.$$

With this and (28), the sequence $\{t_\nu\}$ can be bounded:

$$t_{\nu+1} \leqq t_\nu + 16\sigma^{-2\nu}[\tfrac{1}{2} | x_1 - x_2 | (1 + 4\mu/d)^\nu]^2 d^{-2}.$$

Hence

$$t_{\nu+1} \leqq 4d^{-2}\,|\,x_1 - x_2\,|^2 \sum_{\lambda=0}^{\nu} [(1 + 4\mu/d)/\sigma]^{2\lambda}.$$

Summing this geometrical series,

$$t_\nu/|\,x_1 - x_2\,|^2 \leqq 4d^{-2}\{(\sigma^{-2}(1 + 4\mu/d))^{2\nu+2}/[\sigma^{-2}(1 + 4\mu/d) - 1]\} \equiv \zeta\eta^\nu$$

(definition of ζ, η). Now for any time t, define $\nu(t)$ to be either zero or the integer such that

$$\zeta\eta^{\nu(t)} \leqq t/|\,x_1 - x_2\,|^2 < \zeta\eta^{\nu(t)+1}$$

if this integer exists. Then $t_{\nu(t)} \leqq t$ and $A(t) \leqq A(t_{\nu(t)}) = \sigma^{\nu(t)}$. Also,

$$\nu(t) \geqq (\log(t/\zeta\,|\,x_1 - x_2\,|^2)/\log\eta) - 1.$$

From these observations, we conclude

$$\sigma^{\nu(t)} \leqq \sigma^{-1}\exp[(\log\sigma/\log\eta)\log(t/\zeta\,|\,x_1 - x_2\,|^2)];$$

hence

$$A(t) \leqq \sigma^{-1}(t/\zeta\,|\,x_1 - x_2\,|^2)^{\log\sigma/\log\eta},$$

or

$$\tfrac{1}{2}\int|\,T_1 - T_2\,|\,dx \leqq \sigma^{-1}\zeta^{\alpha/2}(|\,x_1 - x_2\,|/t^{\frac{1}{2}})^\alpha,$$

where $\frac{1}{2}\alpha = -\log\sigma/\log\eta$.

Both σ and η are determined by d. Specifically, $\sigma = 1 - \frac{1}{4}\phi(d)$ and $\eta \doteq [\sigma^{-2}(1 + 4\mu/d)]^2$. An optimal choice of d in relation to $\phi(d)$ would maximize α. We may choose d arbitrarily as, $d^2 = c_1$, say; this will make α a function of μ and c_2/c_1 (proof omitted). In any case, even if we set $d = 1$, we obtain the estimate

$$(29)\qquad \int|\,S(x,t,x_1,t_0) - S(x,t,x_2,t_0)\,| \leqq A_1(|\,x_1 - x_2\,|/(t - t_0)^{\frac{1}{2}})^\alpha,$$

where A_1 and α are a priori constants depending only on n, c_1 and c_2. Also, for the dual adjoint equation,

$$(30)\qquad \int|\,S(x_1,t,x_0,t_0) - S(x_2,t,x_0,t_0)\,|\,dx_0 \leqq A_1(|\,x_1 - x_2\,|/(t - t_0)^{\frac{1}{2}})^\alpha.$$

With (30), we obtain the estimate for the continuity in space of a bounded solution of (1). If $T(x,t)$ satisfies (1) and $|\,T\,| \leqq B$ for $t \geqq t_0$, then

$$\begin{aligned}|\,T(x_1,t) - T(x_2,t)\,| &\leqq |\int[S(x_1,t,x_0,t) - S(x_2,t,x_0,t_0)]T(x_0,t_0)\,dx_0\,| \\ &\leqq B\int|\,S(x_1,t,x_0,t_0) - S(x_2,t,x_0,t_0)\,|\,dx_0.\end{aligned}$$

Hence,

$$(31)\qquad |\,T(x_1,t) - T(x_2,t)\,| \leqq BA_1(|\,x_1 - x_2\,|/(t - t_0)^{\frac{1}{2}})^\alpha.$$

Part V: Time Continuity.

(31) gives half of (2); the remaining part, time continuity, can be derived from (31) and the moment bound (13). Let $T(x,t)$ be a solution of (1) with $|T| \leqq B$ for $t \geqq t_0$. Then for $t' > t > t_0$ we have

$$\begin{aligned} T(x,t) - T(x,t') &= T(x,t) - \int S(x,t',\bar{x},t)\,T(\bar{x},t)\,d\bar{x} \\ &= \int S(x,t',\bar{x},t)\,[T(x,t) - T(\bar{x},t)]\,d\bar{x}, \end{aligned}$$

since $\int S\,d\bar{x} = 1$. Therefore, $|T(x,t) - T(x,t')| \leqq$

$$\begin{aligned} &\int S(x,t',\bar{x},t)\,|T(x,t) - T(\bar{x},t)|\,d\bar{x} \\ &\qquad \leqq \int S(x,t',x+y,t)\,|T(x,t) - T(x+y,t)|\,dy. \end{aligned}$$

Now we separate this integral into two parts, in terms of a radius ρ; one where $|y| \leqq \rho$ and one where $|y| > \rho$. Thus $|T(x,t) - T(x,t')| \leqq I_1 + I_2$, where

$$I_1 = \int_{|y| \leqq \rho} S(x,t',x+y,t)\,|T(x,t) - T(x+y,t)|\,dy \leqq BA_1(\rho/(t-t_0)^{\frac{1}{2}})^{\alpha}$$

(because $\int S\,dy = 1$), and

$$\begin{aligned} I_2 &= \int_{|y|>\rho} S(x,t',x+y,t)\,|T(x,t) - T(x+y,t)|\,dy \\ &\leqq 2B\rho^{-1} \int_{|y|>\rho} |y|\,S(x,t',x+y,t)\,dy \leqq 2B\mu(t'-t)^{\frac{1}{2}}/\rho. \end{aligned}$$

Adding the two inequalities,

$$|T(x,t) - T(x,t')| \leqq BA_1(\rho/(t-t_0)^{\frac{1}{2}})^{\alpha} + 2B\mu(t'-t)^{\frac{1}{2}}/\rho,$$

and if we choose ρ so as to minimize the sum, then

$$\alpha A_1 \rho^{1+\alpha} = 2\mu(t'-t)^{\frac{1}{2}}(t-t_0)^{\frac{1}{2}\alpha},$$

and we obtain

$$|T(x,t) - T(x,t')| \leqq BA_2[(t'-t)/(t-t_0)]^{\frac{1}{2}\alpha/(1+\alpha)}, \tag{32}$$

where $A_2 = (1+\alpha)A_1(2\mu/\alpha A_1)^{\alpha/(1+\alpha)}$. This result (32), combined with (31) yields (2), with $A = \max(A_1, A_2)$.

Part VI: Elliptic Problems.

We treat elliptic problems as a special type of parabolic problem, one in which the coefficients of the equation are time independent and a time independent solution is sought. The Hölder continuity of solutions of uniformly elliptic equations of the form $\nabla \cdot (C \cdot \nabla T) = 0$ appears as a corollary of the result for the parabolic case. There may exist another proof of our result (3). P. R. Garabedian writes from London of a manuscript by Ennio de Giorgi containing such a result. See de Giorgi's note, reference [9].

Let $\mathfrak{D}$ be a domain in space-time defined by the constraints $|x| \leqq \sigma$ and $t \geqq 0$. Then $\mathfrak{D}$ is a solid semi-infinite spherical cylinder. Call $\mathfrak{B}$ the points of the cylindrical surface or boundary of $\mathfrak{D}$, where $|x| = \sigma$. Let $\mathfrak{D}_0$ be the points of the base of $\mathfrak{D}$, where $t = 0$. Define $\mathfrak{B}^*$ as the total boundary of $\mathfrak{D}$, the union $\mathfrak{B} \cup \mathfrak{D}_0$, of the base and cylindrical surfaces.

A "Dirichlet parabolic boundary value problem" is given when values of T are specified on $\mathfrak{B}^*$ and we ask for a solution of (1) in $\mathfrak{D}$ assuming these specified values on $\mathfrak{B}$. The solution of the problem must depend linearly on the boundary values; also, the maximum and minimum principles must hold. These facts require that the solution $T(x,t)$ be determined in this way:

$$T(x,t) = \int T(\xi)\, d\rho(\xi; x, t). \tag{33}$$

Here (x,t) is a point of $\mathfrak{D}$, ξ is any point of $\mathfrak{B}^*$, and $d\rho(\xi; x, t)$ is a positive measure, associated with ξ, which has $\int d\rho = 1$ and which vanishes for $t(\xi) > t$. The time and space coordinates of the point ξ are called $t(\xi)$ and $x(\xi)$. We cannot pause here for a detailed justification of (33), but refer the reader to the literature.

We can define a boundary value problem for which we know the solution in advance by setting $T(\xi) = S(x(\xi), t(\xi), x_0, t_0)$ if $t_0 < 0$. Then the solution of the problem is $S(x, t, x_0, t_0)$, and from (33),

$$S(x, t, x_0, t_0) = \int S(x(\xi), t(\xi), x_0, t_0)\, d\rho(\xi; x, t). \tag{34}$$

This is a powerful identity; it enables us to convert information on fundamental solutions into information on $d\rho$, and in particular, we can obtain a moment bound for $d\rho$. Multiplying (34) by $|x - x_0|$ and integrating, we have

$$\int |x - x_0|\, S(x, t, x_0, t_0)\, dx_0 = \int \int |x - x_0|\, S(x(\xi), t(\xi), x_0, t_0)\, d\rho\, dx_0.$$

Hence

$$\mu(t-t_0)^{\frac{1}{2}} \geqq \int\int\{|x-x(\xi)|-|x_0-x(\xi)|\}S(x(\xi),t(\xi),x_0,t)\,d\rho\,dx_0,$$

so that

$$\mu(t-t_0)^{\frac{1}{2}}+\int\int|x_0-x(\xi)|\,S(x(\xi),t(\xi),x_0,t_0)\,dx_0d\rho$$
$$\geqq \int|x-x(\xi)|\int S(x(\xi),\,t(\xi),x_0,t_0)\,dx_0d\rho.$$

Since $\int S\,dx_0=1$, and from the moment bound (13) again, we obtain

$$\mu(t-t_0)^{\frac{1}{2}}+\int\mu(t(\xi)-t_0)^{\frac{1}{2}}d\rho \geqq \int|x-x(\xi)|\,d\rho.$$

Now $d\rho$ vanishes unless $t(\xi)\leqq t$, and t_0 can be as near to zero as desired; also, $\int d\rho=1$. Hence we can simplify the above to

$$2\mu t^{\frac{1}{2}} \geqq \int|x-x(\xi)|\,d\rho(\xi;x,t). \tag{35}$$

This moment bound (35) on $d\rho$ enables us to control the relative sizes of the effects of the two parts of the boundary in determining $T(x,t)$, where (x,t) is in $\mathcal{D}$. Thus

$$\int|x-x(\xi)|\,d\rho \geqq \int||x|-|x(\xi)||\,d\rho \geqq (\sigma-|x|)\int_{\mathcal{B}}d\rho.$$

Hence

$$\int_{\mathcal{B}}d\rho(\xi;x,t)\leqq 2\mu t^{\frac{1}{2}}/(\sigma-|x|). \tag{36}$$

Now let $T(x)$ be a solution in a region $\mathcal{R}$ of n-space of $\nabla\cdot(C(x)\cdot\nabla T)=0$, where $C(x)$ satisfies the uniform ellipticity condition with bounds c_1 and c_2. If we introduce time and define $T(x,t)=T(x)$, then $T(x,t)$ satisfies $\nabla\cdot(C\cdot\nabla T)=T_t$, which is of our form (1). Suppose x_1 and x_2 are two points of $\mathcal{R}$ and let $d(x_1,x_2)$ be the smaller of $d(x_1)$ and $d(x_2)$, the distances from the boundary of $\mathcal{R}$ of x_1 and x_2 (of course, $d(x_1,x_2)$ may be infinite). For any $\sigma<d(x_1,x_2)$, we can define $\mathcal{D}_1$ as the set of points (x,t) in space-time where $|x-x_1|\leqq\sigma$ and $t\geqq 0$; also, $\mathcal{D}_2$ can be defined for x_2, and the boundaries $\mathcal{B}_1$, $\mathcal{B}_2$, etc. can be defined in the obvious way. $T(x,t)$ can be regarded as a solution of a parabolic boundary value problem either in $\mathcal{D}_1$ or $\mathcal{D}_2$. Another problem with solution $T'(x,t)$ can be defined at first as an initial value problem in all space by setting $T'(x,0)=T(x)$ for all x where $\min(|x-x_1|,|x-x_2|)\leqq\sigma$, that is, $T'(x,t)=T(x)$ when $(x,t)\in\mathcal{D}_{10}\cup\mathcal{D}_{20}$, and setting $T'(x,0)=0$ for all other x values. If $B(\sigma)=\max|T(x)|$ over the set of x values where $\min(|x-x_1|,|x-x_2|)\leqq\sigma$ then $|T'(x,0)|\leqq B(\sigma)$; furthermore, the solution $T'(x,t)$ satisfies $|T'|$

$\leqq B(\sigma)$ for all $t \geqq 0$ by the maximum principle. We can also regard $T'(x,t)$ as a solution of a boundary value problem, either in $\mathcal{D}_1$ or in $\mathcal{D}_2$, where the boundary values are just the values $T'(x(\xi), t(\xi))$ assumed there anyway.

By (33), for any $(x,t) \in \mathcal{D}_i$,

$$T(x,t) - T'(x,t) = \int [T(x(\xi), t(\xi)) - T'(x(\xi), t(\xi))] d\rho_i(\xi; x, t),$$

where $d\rho_i$ is the measure associated with $\mathcal{D}_i$, and $i = 1, 2$. Now $T(x,t) = T(x)$ is time independent, and on $\mathcal{D}_{i0}$ we have $T(x,t) = T'(x,t) = T(x)$. Therefore,

$$|T(x) - T'(x,t)| \leqq \int_{\mathfrak{B}_i} |T(x(\xi)) - T'(x(\xi), t(\xi))| \, d\rho_i \leqq 2B(\sigma) \int_{\mathfrak{B}_i} d\rho_i,$$

and

$$|T(x_i) - T((x_i, t)| \leqq 4B(\sigma)\mu t^{\frac{1}{2}}/\sigma,$$

by use of (36). With our Hölder continuity estimate (2) for solutions of $\nabla \cdot (C \cdot \nabla T) = T_t$ in free space, we can bound $|T'(x_1, t) - T'(x_2, t)|$. This, with the inequality above yields

$$|T(x_1) - T(x_2)| \leqq B(\sigma) A(|x_1 - x_2|/t^{\frac{1}{2}})^{\alpha} + 8\mu B(\sigma) t^{\frac{1}{2}}/\sigma,$$

valid for any positive t. Choice of the optimal t value gives an inequality of the form

$$(37) \qquad |T(x_1) - T(x_2)| \leqq B(\sigma) A'(|x_1 - x_2|/\sigma)^{\alpha/(\alpha+1)}.$$

If $|T(x)| \leqq B$ in $\mathcal{R}$, we may set $\sigma = d(x_1, x_2)$ and obtain (3).

Appendix.

The methods used above can give more explicit results, such as an explicit lower bound for the Hölder exponent α. This takes the form $\alpha = \exp[-a_n(\mu^2/c_1)^{n+1}]$, where a_n depends only on the dimension n. However, a sharper estimate for α might take a quite different form. Numerical calculation of extremal examples might give a better picture.

The moment bound (13) serves to control the rate of dispersal of fundamental solutions. An iterative argument based on (33) and (35) obtains stronger results from (13). In this argument, a fundamental solution is treated as the solution of an array of parabolic boundary value problems, the boundaries being a sequence of spheres centered at the source of the fundamental solution. The result is as follows: let $\nu = [\rho/2\mu(t_2 - t_1)^{\frac{1}{2}}]$, the largest integer not greater than $\rho/2\mu(t_2 - t_1)^{\frac{1}{2}}$, then

$$\int_{|x_2-x_1|\geqq\rho} S(x_2,t_2,x_1,t_1)\,dx_2 \leqq (\pi/4)^{\nu/2}/(\nu/2)\,! \\ \leqq \exp[-\tfrac{1}{2}(\nu+1)\log(2(\nu+1)/\pi e)].$$

Hence,

$$\int_{|x_2-x_1|\geqq\rho} S(x_2,t_2,x_1,t_1)\,dx_2 \\ \leqq \exp\{-\rho\log(\rho/\pi e\mu(t_2-t_1)^{\frac{1}{2}})/4\mu(t_2-t_1)^{\frac{1}{2}}\}. \tag{38}$$

With (38), the reproductive identity (5), and the bound (7), we obtain a pointwise upper bound of the form

$$S(x_2,t_2,x_1,t_1) \\ \leqq k(t_2-t_1)^{-n/2}\exp[-k\,|\,x_1-x_2\,|\,(t_2-t_1)^{-\frac{1}{2}}\log(k\,|\,x_1-x_2\,|\,(t_2-t_1)^{-\frac{1}{2}})]. \tag{39}$$

On the other hand, we obtain from (5) and (23) (or alternatively, from (38) and an analogue of (25)), by an argument resembling that which gave (25), the lower bound

$$S(x_2,t_2,x_1,t_1) \geqq (t_2-t_1)^{-n/2}\phi^*(\,|\,x_1-x_2\,|/(t_2-t_1)^{\frac{1}{2}}), \tag{40}$$

where ϕ^* is an a priori function determined by c_1, c_2, and n. The inequality $S(x_2,t_2,\bar{x},t_1) \geqq P_aP_bP_c$, where

$$P_a = \min S(x_2,t_2,\bar{x},\tfrac{1}{2}(t_1+t_2)) \ \text{ for } \ |\,\bar{x}-x_1\,| \leqq \rho,$$

$$P_b = \min S(\bar{x},\tfrac{1}{2}(t_1+t_2),x_1,t_1) \ \text{ for } \ |\,\bar{x}-x_2\,| \leqq \rho,$$

$$P_c = \int d\bar{x}, \ \text{ where } \ |\,\bar{x}-x_1\,| \leqq \rho \ \text{ and } \ |\,\bar{x}-x_2\,| \leqq \rho,$$

can be used in a iterative argument to strengthen (40). For any $\epsilon > 0$, we obtain

$$S(x_2,t_2,x_1,t_1) \\ \geqq k_1(t_2-t_1)^{-n/2}\exp[-k_2(\,|\,x_1-x_2\,|/(t_2-t_1)^{\frac{1}{2}})^{2+\epsilon}], \tag{41}$$

where k_1 and k_2 depend on ϵ (and on c_1, c_2, and n).

With (38), (41) and (35), we can estimate the speed of convergence to assigned boundary values of the solution of an elliptic boundary value problem, provided the boundary is "tame" enough. A point ξ on the boundary $\mathfrak{B}$ of a region $\mathfrak{R}$ is called *regular* if there are two positive numbers ρ and ϵ such that any sphere with radius $\leqq \rho$ and centered at ξ has at least the fraction ϵ of its volume *not* within $\mathfrak{B}$. Then there are constants D, σ, and β determined by ϵ, c_2/c_1, and n such that for any x in $\mathfrak{R}$ with $|\,x-\xi\,| \leqq \sigma\rho$, we have

$$
\begin{aligned}
&T(x) \geqq \min T(\bar{\xi}) - D\,|(x-\xi)/\rho\,|^{\beta}, \\
&T(x) \leqq \max T(\bar{\xi}) + D\,|(x-\xi)/\rho\,|^{\beta}, \text{ where } |\bar{\xi}-\xi\,| \leqq \rho
\end{aligned}
\tag{42}
$$

($\bar{\xi}$ represents a variable point on the boundary $\mathfrak{B}$).

From (42), it follows that the solution of an elliptic boundary value problem is continuous at the boundary if continuous values were assigned on the boundary and all boundary points are regular. With Hölder continuous boundary values, the solution is Hölder continuous in the region and at the boundary.

From the estimates above, we can fairly easily derive a "Harnack inequality" for parabolic equations:

$$
T(x_2, t) \geqq F(T(x_1, t)/B, |\,x_1 - x_2\,|/(t-t_0)^{\frac{1}{2}}), \tag{43}
$$

provided $0 \leqq T \leqq B$ for $t \geqq t_0$. F is an a priori function, determined by c_1, c_2 and n. For the elliptic case where T is non-negative in a sphere of radius r centered at the origin, the result takes the form

$$
|\log(T(x')/T(x))| \leqq H(r[r-\max(|\,x\,|, |\,x'\,|)]^{-1}, |\,x-x'\,|/r). \tag{44}
$$

The a priori function H is determined by c_2/c_1 and n. This result is less easily obtained than (43).

Parabolic or elliptic problems with Neumann boundary conditions can aparently be handled by a relatively straightforward rederivation of the estimates of this paper in the context of the Neumann boundary, obtaining ultimately the Hölder continuity of the solution for any typical boundary shape.

REFERENCES.

[1] L. Nirenberg, "Estimates and uniqueness of solutions of elliptic equations," *Communications on Pure and Applied Mathematics*, vol. 9 (1956), pp. 509-530.

[2] L. Ahlfors, "On quasi-conformal mapping," *Journal d'Analyse Mathématique*, Jerusalem, vol. 4 (1954), pp. 1-58.

[3] E. Rothe, "Über die Wärmeleitungsgleichung mit nichtkonstanten Koeffizienten in räumlichen Falle I, II," *Mathematische Annalen*, vol. 104 (1931), pp. 340-354, 354-362.

[4] F. G. Dressel, "The fundamental solution of the parabolic equation," (also *ibid.*, II), *Duke Mathematical Journal*, vol. 7 (1940), pp. 186-203; vol. 13 (1946), pp. 61-70.

[5] O. A. Ladyzhenskaya, " On the uniqueness of the Cauchy problem for linear parabolic equations," *Matematičeskiĭ Sbornik*, vol. 27 (69), (1950), pp. 175-184.

[6] F. E. Browder, " Parabolic systems of differential equations with time-dependent coefficients," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 42 (1956), pp. 914-917.

[7] S. D. Eĭdelman, " On fundamental solutions of parabolic systems," *Matematičeskiĭ Sbornik*, vol. 38 (80) (1956), pp. 51-92.

[8] N. Wiener, " The dirichlet problem," *Journal of Mathematics and Physics*, vol. 3 (1924), pp. 127-146.

[9] E. de Giorgi, " Sull'analiticità delle estremali degli integrali multipli," *Atti della Accademia Nazionale dei Lincei*, Ser. 8, vol. 20 (1956), pp. 438-441.

[10] J. Nash, " The embedding problem for Riemannian manifolds," *Annals of Mathematics*, vol. 63 (1956), pp. 20-63.

[11] J. Leray, " Sur le mouvement d'un liquide visqueux emplissant l'espace," *Acta Mathematica*, vol. 63 (1934), pp. 193-248.

[12] C. B. Morrey, Jr., " On the derivation of the equations of hydrodynamics from statistical mechanics," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 279-326.

[13] J. Nash, " results on continuation and uniqueness of fluid flow," *Bulletin of the American Mathematical Society*, vol. 60 (1954), p. 165.

[14] ———, " Parabolic equations," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 43 (1957), pp. 754-758.

THE ALGEBRAIC SIMPLICITY OF CERTAIN GROUPS OF HOMEOMORPHISMS.*

By R. D. Anderson.**

---

1. **Introduction.** In this paper we show that certain groups of transformations of certain strongly setwise homogeneous spaces[1] are algebraically simple. For G a group of the type studied and for $A, B \in G$ with B not the identity, we shall show that A is the product of at most six conjugates[2] of B and B^{-1} (both B and B^{-1} possibly appearing in the same product). The theorem of section 4 asserts conditions under which certain groups can be seen to have this property and hence to be simple. The most interesting type of group to which the conditions are applicable seems to be the group of all homeomorphisms (or, where applicable, of all orientation—preserving homeomorphisms) of a sufficiently setwise homogeneous space. In particular, as corollaries of the theorem of section 4, we conclude that the groups of all homeomorphisms of the Cantor ternary set, the universal curve, the set of all rational numbers, and the set of all irrational numbers are simple. Also the groups of all orientation-preserving homeomorphisms of the universal plane curve, of S^2 (the 2-sphere) and of S^3 (the 3-sphere) are simple. The methods are not applicable to the group of all orientation-preserving homeomorphisms of S^1.[3] Some partial results on the group of all (orientation-preserving) homeomorphisms of S^n are noted at the end of section 3 and in

---

* Received March 4, 1958.

** Presented to the American Mathematical Society, January 29, 1958. The research leading to this paper was supported in part under NSF Grant G-4209.

[1] The space X under examination need not be homogeneous in the usual sense, i. e. for some $A, B \in X$ there need not be a homeomorphism of X onto itself carrying A onto B. But we shall require that there be a collection K of closed subsets of X such that for $k_1, k_2 \in K$, there is a homeomorphism of X onto itself carrying k_1 onto k_2. The precise nature of this "set-wise homogeneity" is given in the definitions to follow of K-structured and (G, K)-rotational.

[2] For $x, y \in G$, $x^{-1}yx$ or xyx^{-1} is called a conjugate of y.

[3] That the group of all orientation preserving homeomorphisms of S^1 is simple was shown by Schreier and Ulam in [6]. Recently Gordon Fisher has observed a modification of the method of argument of the present paper which makes it applicable to the S^1 case and to certain subgroups of the groups of all homeomorphisms of the line.

section 5. The theorem of section 5 asserts that most of the groups of our corollaries (at least) have the additional property that they contain uncountably many conjugate classes.

In 1947, Ulam and von Neumann [7] asserted that the group G of all orientation-preserving homeomorphisms of S^2 was simple and in fact that there exists an $N > 0$ such that if $A, B \in G$ with B not the identity, then A is the product of at most N conjugates of B. In a letter, Ulam has stated that N may be taken as 23. Note that the result of the present paper employs conjugates of both B and B^{-1} and hence does not include this part of the result of [7].

2. Definitions, notation and conventions. All spaces referred to are Hausdorff. Extra conditions of setwise homogeneity will be imposed. Let X denote a space and let G be a group of homeomorphisms of X onto itself. Let $G(X)$ be the group of all homeomorphisms of X onto itself. Let C denote the Cantor ternary set, M the universal curve,[4] N the universal plane curve,[5] Ra the rationals, and let Ir denote the irrationals (on the line).

Let e denote the identity of G, let G^0 be the set of all elements of G which are the identity inside some open subset of X. For $f \in G$ and $k \subset X$, $f \mid k$ denotes the homeomorphism f cut down to k. For $k \subset X$, $\mathrm{Cl}(k)$ denotes the closure of k, $F(k)$ denotes the boundary of k, $I(k)$ denotes $k - F(k)$, and $k^{\sim}$ denotes $X - k$. For $g \in G^0$, any set $k \subset X$ for which $k^{\sim}$ is non-null and $g \mid k^{\sim}$ is $e \mid k^{\sim}$ is said to *support* g or to be a *set of support* for g. For Y any collection of subsets of X, Y^* denotes the union of the elements of Y.

Let K (or $K(X)$ when convenient) be a collection of closed subsets of X. Then X is said to be *K-structured* if

(1) the elements of K are non-degenerate and are homeomorphic to each other,

(2) for $U \subset X$ with U open there exists $k \in K$ such that $k \subset U$,

(3) for $k \in K$, $\mathrm{Cl}(k^{\sim}) \in K$.

---

[4] The universal curve was defined as a 1-dimensional analogue of the Cantor middle third set by punching holes out of a cube. It is characterized in [1] and [2] as a 1-dimensional locally connected continuum with no local cut points and with every open subset containing a 1-skeleton of a 4-simplex.

[5] The universal plane curve N is obtained by punching holes out of a 2-cell so as to get a 1-dimensional set with no local cut points. It is the usual "Swiss cheese" example and is not homogeneous. N contains points p and q (p on a bounding simple closed curve of a complementary domain in the plane and q not so) such that some simple closed curve containing p does not separate N while every simple closed curve containing q does separate N.

Agreement. *We henceforth assume K to exist and X to be K-structured.* Let $\hat{K}$ be the set of images of the elments of K under the various elements of G.

Remark 1. For C, Ra, and Ir, we shall let $K(C)$, $K(Ra)$, and $K(Ir)$ be the sets of all open and closed proper subsets of C, Ra, and Ir, respectively. For S^2 and S^3 we let $K(S^2)$ and $K(S^3)$ be the sets of all closed 2-cells and polyhedral 3-cells in S^2 and S^3 respectively (S^3 being regarded as triangulated). For M, we let $K(M)$ be the set of all closed subsets of M such that for $k \in K(M)$, (1) $I(k)$ and $k^{\sim}$ are connected, (2) $\mathrm{Cl}[I(k)] \cap \mathrm{Cl}(k^{\sim}) = J(k)$ is homeomorphic to C, and (3) no connected subset of $\mathrm{Cl}[I(k)]$ or of $\mathrm{Cl}(k^{\sim})$, open relative to $\mathrm{Cl}(I(k))$ or $\mathrm{Cl}(k^{\sim})$ is disconnected by the omission of $J(k)$. For N, we let $K(N)$ be the collection of all closed sets each bounded by a simple closed curve in N which does not intersect the union of the set of boundaries of the complementary domains of N (as embedded in a plane).

We say that $K' \subset K$ is a *β-sequence* provided (1) K' is a countably infinite collection of disjoint sets with K'^* in the interior of some element of K and (2) $\mathrm{Cl}(K'^*) - K'^*$ is exactly one point $p \in X$ such that every neighborhood of p contains all but a finite number of the elements of K'.

Notation. We shall let $\{k_i\}$, $i = 0, \pm 1, \pm 2, \cdots$, denote a β-sequence and it shall always be assumed that a β-sequence is indexed over all positive, negative and zero integers.

We say that X is *(G,K)-rotational* (or has *(G,K)-rotationality*) provided that for any $k \in K$, there exist a β-sequence $\{k_i\}$ with $\cup k_i \subset k$ and elements $\rho_1, \rho_2 \in G^0$ supported on k such that

(1) $\rho_1(k_i) = k_{i+1}$ for each i,

(2) $\rho_2 \mid k_0$ is $\rho_1 \mid k_0$, $\rho_2 \mid k_{2i}$ is $\rho_1^{-2} \mid k_{2i}$ for $i > 0$, and $\rho_2 \mid k_{2i-1}$ is $\rho_1^{2} \mid k_{2i-1}$ for $i > 0$,

(3) if, for each i, $\varphi_i \in G^0$ is supported on k_i, then there exists $\varphi \in G^0$ supported on $\cup k_i$ such that, for each i, $\varphi \mid k_i$ is $\varphi_i \mid k_i$, and

(4) for any $k' \in K$, there exists $\eta \in G$ such that $\eta(k') = k$.

We say that X is *(G,K)-homogeneous* provided that

(1) X is (G,K)-rotational,

(2) for any $k \in K$ and $g \in G$ for which $g(k) \cap k = \phi$ while $g(k) \cup k \neq X$, there exists $k' \in K$ and $\lambda \in G^0$, with λ supported on k', such that $\lambda \mid k$ is $g \mid k$, and

(3) for any $k_1, k_2, k_3, k_4 \in \hat{K}$ with $k_1 \cap k_2 = k_3 \cap k_4 = \phi$ and $k_1 \cup k_2 \neq X \neq k_3 \cup k_4$, there exists $\mu \in G$ such that $\mu(k_1) = k_3$ and $\mu(k_2) = k_4$.

Remark 2. It is easy to see (or is well known) that for each of C, Ra, Ir, and S^2 and the corresponding previously indicated groups, each space is (G, K)-homogeneous. It follows from results and techniques of [3] that for M and $G(M)$, M is also (G, K)-homogeneous. For G the group of all orientation-preserving homeomorphisms of S^3 and K the set of all polyhedral 3-cells in S^3 (under some triangulation), it follows from results of Bing [5] that S^3 is (G, K)-homogeneous. It follows from results and techniques of [4] and/or rather straightforward arguments that for G the group of all orientation-preserving homeomorphisms of N, N is (G, K)-homogeneous. (That there are orientation-preserving and non-orientation-preserving homeomorphisms of N also follows from [4]).

In Remark 4 of the next section we note that for any $n > 1$, S^n, the n-sphere, K a certain set of n-cells in S^n, and G the group of all (orientation-preserving) homeomorphisms of S^n, S^n is (G, K)-rotational.

Agreement. *In what follows we shall regard $X, K = K(X)$ and G as given with X K-structured and (G, K)-homogeneous unless weaker conditions are explicitly specified. We let h denote an element of G distinct from e. We assume other elements of G to be different from e where appropriate.*

We list some properties of G, K, and X which follow almost immediately from the definitions.

(A) Let m be a subset of X and $g \in G^0$ with g supported on m. Then, for any $\psi \in G$, $\psi^{-1} g \psi$ is supported on $\psi^{-1}(m)$. If $\psi^{-1}(m)$ and m are disjoint, then $f = \psi^{-1} g^{-1} \psi g$ is supported on $m \cup \psi^{-1}(m)$ and $f \mid m$ is $g \mid m$, while $f \mid \psi^{-1}(m)$ is $\psi^{-1} g \psi \mid \psi^{-1}(m)$.

(B) Any conjugate of a product of conjugates of h and h^{-1} is itself a similar product of conjugates of h and h^{-1}; e.g. if

$$f = (g_1{}^{-1} h^{-1} g_1)(g_2{}^{-1} h g_2)(g_3{}^{-1} h^{-1} g_3),$$

then $\varphi^{-1} f \varphi = (\varphi^{-1} g_1{}^{-1} h^{-1} g_1 \varphi)(\varphi^{-1} g_2{}^{-1} h g_2 \varphi)(\varphi^{-1} g_3{}^{-1} h^{-1} g_3 \varphi)$.

(C) For $k_1, k_2 \in \hat{K}$ with $(k_1 \cup k_2)^{\sim} \neq \phi$, there exists a $k \in K$ such that $k_1 \cup k_2 \subset I(k)$. Note that as $(k_1 \cup k_2)^{\sim}$ is open, there exists a $k' \subset (k_1 \cup k_2)^{\sim}$, and $\mathrm{Cl}(k'^{\sim}) \in K$).

(D) X has no isolated points and each element of K is infinite.

(E) If $\alpha, \beta, \gamma \in G$ and m is any closed set in X, then in studying the action of $f = \alpha\beta\gamma$ on m we first look at γ on m, then at β on $\gamma(m)$ and finally at α on $\beta(\gamma(m))$.

3. Lemmas and theorems.

In Theorem I and Lemma 1, we note consequences of (G, K)-rotationality of X (without requiring (G, K)-homogeneity).

THEOREM I. *Let X be (G, K)-rotational. For $g \in G^0$, g is the product of four conjugates of h and h^{-1} (appearing alternately).*

We first note that Theorem I follows from

LEMMA 1. *Let X be (G, K)-rotational. There exists $k_0 \in K$ such that for any $g_0 \in G^0$ with g_0 supported on k_0, g_0 is the product of four conjugates of h and h^{-1} (appearing alternately).*

For $g \in G^0$, g is supported on some element k of K. By condition (4) of (G, K)-rotationality, there exists an $\alpha \in G$ such that $\alpha(k)$ is k_0. Then $\alpha g \alpha^{-1} = g_0$ is supported on k_0 and $g = \alpha^{-1} g_0 \alpha$. Thus, by Note (B), as g_0 is the product of four conjugates of h and h^{-1} (alternately), so is g.

Proof of Lemma 1. Let $k \in K$ such that $k \cap [h(k) \cup h^{-1}(k)] = \phi$. That such a k exists follows from the existence of some p for which $h(p) \neq p$, property (2) of K-structured, and the continuity of h and h^{-1}. Let $\{k_i\}$ be a β-sequence with $\cup k_i \subset k$ and $\rho_1, \rho_2 \in G^0$ existing as in the definition of (G, K)-rotationality. The k_0 introduced here is to be the k_0 of the lemma. Let φ_i be $\rho_1{}^i g_0 \rho_1{}^{-i}$, $i \geqq 0$. By condition (3) of (G, K)-rotationality, there exists $\varphi \in G^0$ such that φ is supported on $\cup k_i$, $i \geqq 0$, $\varphi \mid k_0$ is $g_0 \mid k_0$, $\varphi \mid k_i$ is $e \mid k_i$, $i < 0$, and $\varphi \mid k_i$ is $\rho_1{}^i g_0 \rho_1{}^{-i} \mid k_i$ is $\varphi_i \mid k_i$ for $i > 0$.

Consider $f = h^{-1}\varphi^{-1}h\varphi$. By note A, f is supported on $[\cup k_i] \cup [\cup h^{-1}(k_i)]$ for $i \geqq 0$. Furthermore, $f \mid k$ is $\varphi \mid k$, whereas $f \mid h^{-1}(k)$ is $h^{-1}\varphi^{-1}h \mid h^{-1}(k)$. Let $\rho = (h^{-1}\rho_2 h)\rho_1{}^{-1}$. Then ρ is $\rho_1{}^{-1}$ over k and is $h^{-1}\rho_2 h$ over $h^{-1}(k)$.

Let

$$w = \rho^{-1} f^{-1} \rho f = \rho^{-1}\varphi^{-1}h^{-1}\varphi h \rho h^{-1}\varphi^{-1}h\varphi = (\rho^{-1}\varphi^{-1}h^{-1}\varphi\rho)(\rho^{-1}h\rho)(h^{-1})(\varphi^{-1}h\varphi).$$

Thus w is the product of four conjugates of h and h^{-1} (alternately).

We wish to check that w is g_0 and hence prove the lemma. To do so, we need merely track down the action of w on various subsets of X.

As f is supported on $Y = [\cup k_i] \cup [\cup h^{-1}(k_i)]$ for $i \geqq 0$, then clearly as $Y \subset \rho(Y)$, $w = \rho^{-1} f^{-1} \rho f$ is supported on Y. Each of f and ρ is the product of two elements of G^0, one supported on k and the other on $h^{-1}(k)$. Therefore, we may consider the effect of w on k and $h^{-1}(k)$ separately in terms of those factors which are supported on k and $h^{-1}(k)$ respectively. Thus $w \mid k$ is $\rho_1\varphi^{-1}\rho_1^{-1}\varphi \mid k$ and $w \mid h^{-1}(k)$ is $(h^{-1}\rho_2^{-1}h)(h^{-1}\varphi h)(h^{-1}\rho_2 h)(h^{-1}\varphi^{-1}h) \mid h^{-1}(k)$.

We look first at $w \mid k$. As noted above, w is supported on $\cup\, k_i$, $i \geqq 0$. But $w \mid k_0$ is $\varphi \mid k_0$ is $g_0 \mid k_0$, for $\rho_1\varphi^{-1}\rho_1^{-1} \mid k_0$ is $e \mid k_0$. Now for $i > 0$, $w \mid k_i$ is $\rho_1\varphi^{-1}\rho_1^{-1}\varphi \mid k_i$ is

$$\rho_1(\rho_1{}^{i-1}g_0{}^{-1}\rho_1{}^{-i+1})\rho_1{}^{-1}(\rho_1{}^{i}g_0\rho_1{}^{-i}) \mid k_i \text{ is } \rho_1{}^{i}g_0{}^{-1}g_0\rho_1{}^{-i} \mid k_i$$

is $e \mid k_i$. We use property E here (and later). Thus $w \mid k$ is $g_0 \mid k$.

Finally, we look at $w \mid h^{-1}(k)$. By cancelling hh^{-1} where applicable, we note that $w \mid h^{-1}(k)$ is $h^{-1}\rho_2{}^{-1}\varphi\rho_2\varphi^{-1}h \mid h^{-1}(k)$, and to show that $w \mid h^{-1}(k)$ is $e \mid h^{-1}(k)$, we need merely show that $\rho_2{}^{-1}\varphi\rho_2\varphi^{-1} \mid k$ is $e \mid k$. Now $\varphi^{-1} \mid k_0 = g_0{}^{-1} \mid k_0$ and for $i > 0$, $\varphi^{-1} \mid k_i$ is $\rho_1{}^{i}g_0{}^{-1}\rho_1{}^{-i} \mid k_i$. Hence for $i > 0$, $\rho_2{}^{-1}\varphi\rho_2\varphi^{-1} \mid k_{2i}$ is $\rho_1{}^{2}(\rho_1{}^{2i-2}g_0\rho_1{}^{-2i+2})\rho_1{}^{-2}(\rho_1{}^{2i}g_0{}^{-1}\rho_1{}^{-2i}) \mid k_{2i} = e \mid k_{2i}$, $\rho_2{}^{-1}\varphi\rho_2\varphi^{-1} \mid k_{2i-1}$ is

$$\rho_1{}^{-2}(\rho_1{}^{2i+1}g_0\rho_1{}^{-2i-1})\rho_1{}^{2}(\rho_1{}^{2i-1}g_0{}^{-1}\rho_1{}^{-2i+1}) \mid k_{2i-1}$$

is $e \mid k_{2i-1}$, and for $i = 0$, $\rho_2{}^{-1}\varphi\rho_2\varphi^{-1} \mid k_0$ is $\rho_1{}^{-1}(\rho_1 g_0\rho_1{}^{-1})\rho_1 g_0{}^{-1} \mid k_0 = e \mid k_0$.

Thus Lemma 1 and Theorem I are established.

THEOREM II. *Let X be (G,K)-homogeneous. For any $k, k' \in K$ with $k \cap k' = \phi$ and $k \cup k' \neq X$ and for any $g \in G^0$ with g supported on k, there exists an $f \in G^0$ such that $f \mid k$ is $g \mid k$, $f \mid (k \cup k')^{\sim}$ is $e \mid (k \cup k')^{\sim}$ and f is the product of a conjugate of h and a conjugate of h^{-1}.*

We first note that Theorem II follows from

LEMMA 2. *Let X be (G,K)-homogeneous. For some $k_0, k_0' \in K$, $k_0 \cap k_0' = \phi$ and $k_0 \cup k_0' \neq X$, and for any $g_0 \in G$ with g_0 supported on k_0, there exists an $f_0 \in G^0$ such that $f_0 \mid k_0$ is $g_0 \mid k_0$, $f \mid (k_0 \cup k_0)^{\sim}$ is $e \mid (k_0 \cup k_0')^{\sim}$ and f is the product of a conjugate of h and a conjugate of h^{-1}.*

Assume Lemma 2. By condition (3) of (G,K)-homogeneity, there exists $\mu \in G$ such that $\mu(k_0) = k$ and $(k_0') = k'$. Let $g_0 \mid k_0$ be $\mu^{-1}g\mu \mid k_0$. Let f_0 be as in Lemma 2. Then $f = \mu f_0\mu^{-1}$ satisfies the conditions of the theorem.

Proof of Lemma 2. Let $k_0 \in K$ such that $k_0 \cap [h(k_0) \cup h^{-1}(k_0)] = \phi$. Let $g_0 \in G_0$ with support on k_0. Then $f_0 = h^{-1}g_0{}^{-1}hg_0$ satisfies the conditions of the lemma with $k_0' = h^{-1}(k_0)$.

Remark 3. The order for the product of Theorem II could (by appropriate modification of the argument) be taken either as h, h^{-1} or as h^{-1}, h.

Remark 4. We suggest a construction which enables us to observe that if X is S^n, $n > 1$, and G is the group of all (orientation-preserving) homeomorphisms of S^n, there exists a K with respect to which X is K-structured and (G, K)-rotational.

We regard S^n as the one-point compactification of Euclidean n-space E^n. Let K be the set of (a) those closed n-cubes in E^n whose faces are parallel to the coordinate planes and (b) the closures of the complements of those n-cubes. Let $k \in K$ with center at the origin and edge of large size. Let now $\{k_i\}$ be a β-sequence with $\cup k_i \subset k$ such that k_0 has its center at $(1, 0, 0, \cdots, 0)$ whereas k_i, for $i < 0$, has its center at $(1/2^i, -1/2^i, 0, 0, \cdots, 0)$, k_{2i}, $i \geqq 0$, has its center at $(1/2^{2i}, 1/2^{2i}, 1/2^{2i}, 0, 0, \cdots, 0)$, while k_{2i-1}, $i > 0$, has its center at $(1/^{2i-1}, 1/^{2i-1}, -1/^{2i-1}, 0, 0, \cdots, 0)$. Now it is clear that a ρ_1 can be defined as in the definition of (G, K)-rotational with the added provision that ρ_1 preserves geometric orientation and direction on each k_i. But then, similarly, it is clear that ρ_2 as in the definition can also be defined and hence S^n is (G, K)-rotational.

4. The main theorem and its corollaries.

THEOREM III. *Let X be (G, K)-homogeneous. Then for $g \in G$, g is the product of six conjugates of h and h^{-1} (written alternately or in the order $h, h^{-1}, h^{-1}, h, h^{-1}, h$) and hence G is simple.*

Proof. We use condition (2) of (G, K)-homogeneity (not previously employed). It is here that the orientation-preserving condition of certain groups becomes significant. Let $k \in K$ such that $g(k) \cap k = \phi$ and $g(k) \cup k \neq X$. Let $k' \in K$ for which $I(k') \supset k \cup g(k)$. Let $\alpha \in G^0$ supported on k' such that $\alpha \mid k$ is $g \mid k$. Then as $\alpha, (\alpha^{-1}g) \in G^0$ and $\alpha(\alpha^{-1}g) = g$, it follows from Theorem I that g can be written as the product of eight conjugates of h and h^{-1}. We sharpen this result slightly to get Theorem III. Let $k'' \cap k' = \phi$ and $k'' \cup k' \neq X$. By Theorem II, there is a $\beta \in G^0$ supported on k'' such that $\alpha\beta$ is the product of a conjugate of h and one of h^{-1} (in either order). Hence as $(\beta^{-1}\alpha^{-1}g) \in G^0$ and $(\alpha\beta)(\beta^{-1}\alpha^{-1}g) = g$, the theorem follows from Theorem I.

Noting Remarks 1 and 2, the following corollaries are immediate consequences of Theorem III.

COROLLARY 1. *If G is the group of all orientation-preserving homeomorphisms of N, S^2 or S^3 and $h \in G$ with $h \neq e$, then G is simple, and in fact, each element of G is the product of six conjugates of h and h^{-1}.*

COROLLARY 2. *If G is the group of all homeomorphisms of the Cantor set C, the universal curve M, the rationals Ra or the irrationals Ir and $h \in G$ with $h \neq e$, then G is simple, and in fact,, each element of G is the product of six conjugates of h and h^{-1}.*

5. Conjugate classes. We give conditions on G sufficient to establish that G have uncountably many conjugate classes and we note that the groups of the corollaries of the last section as well as the group of orientation preserving homeomorphisms of S^n, $n > 1$, satisfy these conditions (except for the groups associated with M and N for which this argument is not designed).

Suppose that for some $k, k' \in K$ with $k' \subset k$ and for each $i > 1$, there exists a $g_i \in G$ such that

(1) g_i is supported on k,

(2) g_i is of period i on k', and

(3) g_i is not of period $j, j \neq 1, i$, on any homeomorph of k' different from k'. Then we say that G is *w-locally periodic.*

THEOREM IV. *If X is (G, K)-rotational and G is w-locally periodic, then G contains uncountably many distinct conjugate classes.*

Proof. Let $\hat{k} \in K$, let $\{k_i\}$ be a β-sequence with $\cup k_i \subset \hat{k}$ and let $\rho_1 \in G^0$ as in the definition of (G, K)-rotational such that ρ_1 is supported on $\hat{k}$ and for each i, $\rho_1(k_i) = k_{i+1}$. Let k and k' be as in the definition of w-locally periodic. Let $\sigma \in G$ such that $\sigma(k) = k_0$. Then for each i, $\sigma g_i \sigma^{-1}$ satisfies the conditions of periodicity above with respect to k_0 and $\sigma(k') = k_0'$. For $i > 0$, let $\varphi_i = \rho_1{}^i \sigma g_i \sigma^{-1} \rho_1{}^{-i}$. For each proper subsequence α of the positive primes let $\varphi_\alpha \in G$ which (1) is supported on $\cup k_i$, $i \in \alpha$, and (2) is φ_i over k_i for $i \in \alpha$. There are uncountably many (in fact, continuum-wise many) such sequences α. But for the distinct subsequences α and β of the positive primes, we show that φ_α and φ_β are not conjugate to each other. Without loss of generality, suppose φ_α is periodic with period p over some $k^0 \in K$ while φ_β is not periodic with period p over any homeomorphic image of an element of K. Suppose $\varphi_\alpha = f^{-1}\varphi_\beta f$; then $\varphi_\alpha{}^p$ is $(f^{-1}\varphi_\beta f)^p$ is $f^{-1}\varphi_\beta{}^p f$ which implies a contradiction.

LOUISIANA STATE UNIVERSITY.

REFERENCES.

[1] R. D. Anderson, "A characterization of the universal curve and a proof of its homogeneity," *Annals of Mathematics*, vol. 67 (1958), pp. 313-324.

[2] ———, "One-dimensional continuous curves and a homogeneity theorem," to be published in the *Annals of Mathematics*.

[3] ———, "On homogeneity and extending homeomorphisms in universal curves," to be submitted.

[4] ———, "On certain one-dimensional continuous curves," to be published in the *Canadian Journal of Mathematics*.

[5] R. H. Bing, "Locally tame sets are tame," *Annals of Mathematics*, vol. 59 (1954), pp. 145-158.

[6] J. Schreier and S. Ulam, "Eine Bemerkung über die Gruppe der topologischen Abbildüngen der Kreislinie auf sich selbst," *Studia Mathematica*, vol. 5 (1935), pp. 155-159.

[7] S. M. Ulam and J. von Neumann, "On the group of homomorphisms of the surface of the sphere," (abstract), *Bulletin of the American Mathmaetical Society*, vol. 53 (1947), p. 506.

APPLICATIONS OF THE THEORY OF MORSE TO SYMMETRIC SPACES.*

By RAOUL BOTT [1] and HANS SAMELSON.[2]

To Marston Morse on his 65th birthday.

Introduction. In this sequel to [6], we bring the proof of results announced in [7] and [8]. Although [6] might be a good introduction, the present paper is relatively self contained.

Let Ω be the loop space on the connected compact Lie group K, and let S be the set of geodesics on K leading from a general point P to the identity e. (A point of K is general if it is contained in only one maximal torus of K.) To each $s \in S$ we assign an index (dimension), δ_s, equal to the number of (properly counted) singular points of K in the interior of s. The main result of [6] then states that $H_*(\Omega; \mathbf{Z})$ is *abstractly* isomorphic to S_*, the free module generated by the elements of S, and graded by the index δ. (Thus as a generator in S_*, the element $s \in S$ has dimension δ_s.)

In the present paper this result is extended in two ways: a) We define an explicit isomorphism $\gamma\colon S_* \to H_*(\Omega; \mathbf{Z})$; in other words, we describe a base of singular cycles for $H_*(\Omega; \mathbf{Z})$. b) We show that (at least with $\mathbf{Z}_2$ as coefficients) a completely analogous description of $H_*(\Omega)$ holds in several instances, notably when Ω is the loopspace of a symmetric space.

This program is carried out in chapters I and II. We start by constructing a homomorphism $\gamma\colon S_* \to H_*(\Omega)$ (at least mod 2) under rather general conditions: Ω is the loop space of a manifold M on which a compact Lie group K acts with at least one fixed point. The set S is now defined as above, with the fixed point playing the role of e and P being any point on a K-orbit of maximal dimension. The index $\delta_K(s)$ is computed again as before, the K-singular points of M being the points on lower-dimensional orbits. Using the K-singular points in s, we construct a manifold Γ_s (with $\dim \Gamma_s = \delta_K(s)$) and a homeomorphism $f_s\colon \Gamma_s \to \Omega$, for each $s \in S$. These sub-

---

* Received March 5, 1958.

[1] Work supported in part by the A. P. Sloan Foundation.

[2] Work supported in part by Air Force Contract AF 49(638)-104.

manifolds of Ω can be thought of as generalizations of the cycles in the loop space of a sphere which Morse constructed (cf. [16]). By assigning to each $s \in S$ the f_s-image of the fundamental cycle on Γ_s, we obtain the homomorphism $\gamma: S_* \rightarrow H_*(\Omega)$, in general mod 2, and over the integers if all the Γ_s are orientable. The details of this construction are given in Chapter I, nos. 1-5.

In general this homomorphism has no great virtue. However, and this is our main observation, if the action of K on M satisfies a certain infinitesimal condition, already introduced in [6] and there called variational completeness, then $\gamma: S_* \rightarrow H_*(\Omega)$ is an isomorphism onto. This is the content of Theorem I.

Intuitively, we like to think of variational completeness as absence of conjugate points on the decomposition space M/K. This is literally correct when K reduces to the identity, or $M \rightarrow M/K$ is a fibering. In the case of K acting on itself by inner automorphisms, this interpretation fits in with E. Cartan's description of this decomposition space as a Euclidean cell (with certain identifications on the boundary); the proof that variational completeness holds for this example was already given in [6].

The proof of Theorem I takes up the rest of Chapter I. The Morse theory enters vitally, and more delicately than in [5], where one merely applied the Morse inequalities.

In Chapter II, we prove that variational completeness holds in various instances (Theorem II). All of these cases are associated with symmetric spaces.

In Chapter III, we describe the ring $H^*(\Gamma_s; \mathbf{Z})$ for a generic s on the group K, in terms of the Cartan integers of K (Proposition 4.2). The rest of that chapter then is devoted to applications, of Theorem I and this description of $H^*(\Gamma_s)$, to the topology of Lie groups. The main results are outlined in no. 2 of that chapter. We have reproduced our computations with possibly greater detail than is currently the custom.

Chapter IV contains immediate applications of Theorems I and II to symmetric spaces in general. The results here are less complete than in Chapter III. The manifolds Γ_s need not be orientable so that we have to restrict ourselves to the coefficient domain $\mathbf{Z}_2$. We do not know whether the loopspace of a general symmetric space has ony two-torsion.

Chapter I. Action of a Group and the Theory of Morse.

1. Action of a group on a manifold. All manifolds considered in this paper are of class C^∞. They are not necessarily connected, but all components of a manifold are of the same dimension. If x is a point of the manifold M, then M_x denotes the tangent space of M at x. If $f\colon M \to M'$ is a map (always C^∞) of the manifold M into the manifold M', then $\dot{f}_x\colon M_x \to M'_{x'}$ denotes the differential of f at x, with $x' = f(x)$. If f is a curve in M, i.e. a map of the real line $E^1 = \mathbf{R}$ into M, we write $\dot{f}(t)$ for the tangent vector to f at t, that is, for the image under $\dot{f}_t$ of the standard tangent vector D_t (or $\frac{d}{dt}$) of E^1 at t.

Let K be a compact Lie group, and M a (paracompact) manifold of dimension r. *Let K act on M from the left,* i.e. *let there be given a map*

$$\pi\colon K \times M \to M \text{ of class } C^\infty \tag{1.1}$$

such that (with $\pi(k,x)$ abbreviated to $k\cdot x$) *the following conditions hold:*

$$e\cdot x = x, \text{ where } e \text{ is the identity of } K; \tag{1.2}$$

$$k\cdot(k'\cdot x) = (k\cdot k')\cdot x \text{ for } k, k' \in K, x \in M. \tag{1.3}$$

The K-orbit of a subset A is denoted by $K\cdot A$. Thus,

$$K\cdot A = \{k\cdot a\colon k \in K, a \in A\}. \tag{1.4}$$

The stabilizer (stability group) of A is denoted by K_A; this is the subgroup of K which keeps A pointwise fixed,

$$K_A = \{k \in K\colon k\cdot a = a, a \in A\}. \tag{1.5}$$

For each $x \in M$, the orbit $K\cdot x$ is a regular submanifold of M, C^∞-homeomorphic to the quotient space K/K_x.

It is also convenient to denote, for any $k \in K$, by $\pi_k\colon M \to M$ the map defined by $\pi_k(x) = k\cdot x$, and to abbreviate $\pi_k \circ f$ to $k\cdot f$, for any map f with values in M.

It is well known that M can be given a Riemannian metric that is invariant under the action of K, so that all the maps $\pi_k\colon M \to M$ become isometries. We assume that such a metric is assigned, and use the notation (X, Y) for the corresponding inner product of two vectors in M_x; the norm of X is written $|X|$.

The action of K on M induces a representation of the Lie algebra $\mathfrak{k}$ of

K by vector fields over M. These vector fields—the infinitesimal K-motions—can be defined in the following manner:

Let X be an element of $\mathfrak{k}$, and let $h: \boldsymbol{R} \to K$ be the corresponding 1-parameter subgroup, with $\dot{h}(0) = X$.

DEFINITION 1.6. *For $x \in M$, let $h_x: R \to M$ be the curve defined by $h_x(\alpha) = h(\alpha) \cdot x$ for any $\alpha \in \boldsymbol{R}$. The assignment $x \to \dot{h}_x(0)$ defines a vector field $\bar{X}$ on M, which is called the infinitesimal K-motion corresponding to X.*

It is clear that the tangent space to the K-orbit $K \cdot x$ at x is given by the values of all possible infinitesimal K-motions at x:

$$(K \cdot x)_x = \{\bar{X}(x) : X \in \mathfrak{k}\}. \tag{1.7}$$

The Riemannian metric in M defines in standard fashion the concept of distance (greatest lower bounds of length of curves connecting the two points), and the concept of geodesic. To be able to apply the theory of Morse, we shall assume that M is complete under its metric, so that geodesics can be continued indefinitely in both directions. A geodesic will then always be a non-degenerate C^∞-map of $\boldsymbol{R}$ into M, satisfying the usual differential equations for geodesics, parametrized proportionally to arc length. A geodesic segment s is the restriction of a geodesic g to an interval $[a, b]$ with $a < b$. The point $s(a)$ is the initial point, $s(b)$ is the terminal point of s. We write K_s for the stabilizer of $s([a, b])$; similarly for the stabilizer of a geodesic. The elements of K map geodesics into geodesics (the maps π_k are isometries).

2. K-transversality; the space $\boldsymbol{\Omega}(M; R, N)$.

We introduce some basic definitions.

DEFINITION 2.1. *A geodesic g of M is called K-transversal (briefly: transversal) if for each $t \in \boldsymbol{R}$ the tangent vector $\dot{g}(t)$ is orthogonal to the K-orbit of the point $g(t)$ (i.e., orthogonal to the tangent space of the submanifold $K \cdot g(t)$ of M at $g(t)$); similarly for geodesic segments.*

There exist many transversal geodesics (unless K is transitive on M, in which case there are none at all!), as the next proposition shows.

PROPOSITION 2.2. *The geodesic g is transversal if there exists a $t_0 \in \boldsymbol{R}$ such that $\dot{g}(t_0)$ is orthogonal to $K \cdot g(t_0)$.*

In other words, transversality holds, provided it holds at a single point. The proof of Proposition 2.2 is an immediate consequence of Gauss' theorem on orthogonal trajectories of families of geodesics; we will give it in no. 6.

DEFINITION 2.3 (cf. [6], Def. 5.1). *If* A, B *are subsets of* M, *then* $\Omega(M;A,B)$ *denotes the metric space of all piecewise regular curves (maps* u *of the unit interval* $[0,1]$*) in* M *from* A *to* B, *i.e. with* $u(0) \in A$, $u(1) \in B$, *parametrized proportionally to arc length, with the distance between two curves* u *and* u' *defined as*

$$\sup_{t \in [0,1]} d(u(t), u'(t)) + |(L(u) - L(u')|;$$

here d *is the distance in* M, *and* L *denotes the length of the curves.*

Note that L is a continuous function on $\Omega(M;A,B)$.

Remark. The set $\Omega(M;A,B)$ is contained in the set $\Omega'(M;A,B)$ of all continuous curves (maps of $[0,1]$ into M) from A to B; if the latter, as customary, is topologized by the compact-open topology, then the inclusion map is continuous, and induces an isomorphism of the singular homology groups and also of the homotopy groups of the two spaces [17].

Let R be a point of M, and let N be the K-orbit of a point of M; to avoid trivial complications, assume $R \notin N$. The main object of study in this paper will be the space $\Omega = \Omega(M;R,N)$, to which we shall apply the theory of Morse. The next definition introduces a subset of Ω that is basic for this application.

DEFINITION 2.4. $S = S(M;R,N)$ *is the set of transversal geodesic segments, parametrized (proportionally to arc length) on* $[0,1]$, *from* R *to* N, *i.e. with initial point* R *and with terminal point on* N.

3. Fiber bundle concepts. We interpolate a section recalling some concepts from the theory of fiber bundles, specialized slightly to fit our purposes. By a principal bundle E for a compact Lie group G (the structure group) we mean a compact manifold on which G acts, from the right, without fixed points ($p \cdot g = p \Rightarrow g = e$). The decomposition space of E, derived from the decomposition of E into the orbits under G, is the base space B, a manifold. The natural map of E onto B is called the projection; it is differentiable; only the vectors tangent to the fibers are mapped into 0. One often writes E/G for B, particularly in the case where E is a group, G a subgroup and $B = E/G$ the space of left cosets of G.

We describe the standard construction of fiber spaces, associated to the principal bundle E for G: Suppose G operates, from the left, on another space F. The product of E and F over G, written $E \times_G F$, is obtained by identifying $(p \cdot g, x)$ with $(p, g \cdot x)$ in $E \times F$, or equivalently, by letting G

act on $E \times F$ via $(p,x) \cdot g = (p \cdot g, g^{-1} \cdot x)$ (which makes $E \times F$ into a principal G-bundle) and taking the base space. There exists a map of $E \times_G F$ onto B which makes the following diagram commutative:

(3.1)
$$\begin{tikzcd} E \times F \arrow[r] \arrow[d] & E \arrow[d] \\ E \times_G F \arrow[r] & B, \end{tikzcd}$$

where the other maps are the natural ones; this map is the induced fiber map with F as fiber.

Let another group G' act principally on F from the right, such that the actions of G and G' on F associate, and let G' act from the left on a third space F'. Then $E \times F \times F'$ is a principal $G \times G'$-bundle by the definition $(p,x,x') \cdot (g,g') = (p \cdot g, g^{-1} \cdot x \cdot g', g'^{-1} \cdot x')$. The base space, denoted by $E \times_G F \times_{G'} F'$, can in an obvious way be regarded also as $E \times_G (F \times_{G'} F')$ or $(E \times_G F) \times_{G'} F'$. Extension to more factors is immediate. Similarly, the two spaces $E \times_G F/G'$ and $(E \times_G F)/G'$ can be identified.

Let E, E' be two principal bundles with structure groups G, G' and base spaces B, B'. A map $\bar{f}\colon E \rightarrow E'$ is a bundle map or equivariant map relative to a homomorphism $f\colon G \rightarrow G'$, if $\bar{f}(p \cdot g) = \bar{f}(p) \cdot f(g)$ for $p \in E$, $g \in G$. Such a map induces a map $\bar{f}$ of B into B'. The spectral sequence of E (in homology) is then mapped into that of E'; the map has the obvious naturality properties with respect to E_2, and the transgression (cf. [18] for these concepts).

4. The K-cycle of a geodesic segment. Let $s\colon [0,1] \rightarrow M$ be an element of the set S (cf. (2.4)), i.e. a transversal geodesic segment with $s(0) = R$ and $s(1) \in N$. We shall attach to s a manifold Γ_s, the "K-cycle of s," and a homeomorphism f_s of Γ_s into Ω. We first describe Γ_s abstractly, and present its geometrical meaning in the next section.

DEFINITION 4.1. *The parameter value* $t \in [0,1)$ (*note that* 1 *is excluded*) *and the point* $s(t)$ *are called exceptional for* s, *if for the dimensions of the stabilizers* $K_{s(t)}$ *and* K_s (cf. no. 1), *the relation*

$$\dim K_{s(t)} > \dim K_s$$

holds.

Geometrically, the exceptional points are those where the segment encounters orbits of lower dimension. We shall show in (9.2) that each s has only a finite number of exceptional values, and that the exceptional values are related to the focal values.

Let $t_1 < t_2 < \cdots < t_n$ be the exceptional values of s; the stabilizers $K_{s(t_i)}$ are then defined, and we put, for brevity [as long as we consider a fixed s]:

(4.2) $$K_i = K_{s(t_i)}, \qquad i = 1, \cdots, n.$$

The stabilizer K_s of the whole segment s is a subgroup of each K_i; it acts on K_i principally from the left and the right, by multiplication, and acts also from the left on the coset space K_n/K_s. Because of the importance of coset spaces with K_s as subgroup, we introduce the following notation:

(4.3) *If G is a group containing K_s, then G^s denotes the left coset space G/K_s.*

In the following fundamental definition, we make use of the notation introduced in no. 3.

DEFINITION 4.4. *The K-cycle of s, denoted by Γ_s, is the manifold*

$$K_1 \times_{K_s} K_2 \times_{K_s} \cdots \times_{K_s} K_{n-1} \times_{K_s} K_n{}^s;$$

note that the last factor, according to (4.3), is K_n/K_s.

The dimension of Γ_s is given by

(4.5) $$\dim \Gamma_s = \sum_i (\dim K_i - \dim K_s).$$

If s has no exceptional values at all, we let Γ_s be a single point.

The manifold Γ_s can also be considered as the base space of $K_1 \times_{K_s} K_2 \times_{K_s} \cdots \times_{K_s} K_n$, under the right operation of K_s on K_n. A third description will be used below. Put

(4.6) $$W_s = K_1 \times \cdots \times K_n,$$

and let the n-th power $(K_s)^n = K_s \times \cdots \times K_s$ operate on W_s by the rule

(4.7) $$p \cdot q = (c_1 a_1, a_1^{-1} c_2 a_2, a_2^{-1} c_3 a_3, \cdots, a_{n-1}^{-1} c_n a_n)$$

for $p = (c_1, \cdots, c_n) \in W_s$, $q = (a_1, \cdots, a_n) \in (K_s)^n$.

One verifies that this is a principal bundle operation, and that the base space is exactly Γ_s. We denote by ψ_s the projection of W_s onto Γ_s. It should be noted that although $(K_s)^n$ is a subgroup of W_s, and although the orbit of the point $(e, \cdots, e)$ of W_s under the operation (4.7) is just $(K_s)^n$, the operation (4.7) is not identical with left (or right) group multiplication in W_s, and Γ_s is not homeomorphic with the coset space $W_s/(K_s)^n$; it is easily seen, however, that the two spaces have isomorphic homotopy groups π_i for $i > 1$, and that they agree in π_1 up to an extension.

For an example, let M be the 2-sphere $\{x\colon x_1{}^2+x_2{}^2+x_3{}^2=1\}$ in 3-space, and let K, isomorphic to the circle group S_1, be the group of rotations around the x_3-axis. Let $R=(1,0,0)$; $N=\{(0,0,1)\}$. Let s be the geodesic segment from $(1,0,0)$ to the southpole $(0,0,-1)$ to $(-1,0,0)$ to the northpole $(0,0,1)$. There is one exceptional value, $t=\frac{1}{3}$. The stabilizer K_1 is equal to K, the stabilizer K_s reduces to the identity. We have $\Gamma_s=W_s=K$, a circle.

5. Geometric form of the K-cycles. We come to the concrete representation of Γ_s as a submanifold of the path space Ω (cf. no. 2). Let again $t_1<t_2<\cdots<t_n$ be the exceptional t-values for s. Put $t_0=0$, $t_{n-1}=1$, and denote by s_i the restriction of s to $[t_i,t_{i+1}]$, for $i=0,\cdots,n$; the first one of these is possibly a single point, the others are non-degenerate geodesic segments. We write

$$s=s_0+s_1+\cdots+s_n \tag{5.1}$$

for this decomposition of s. With its help, we shall define a map $\bar{f}_s$ of the manifold W_s (cf. (4.6)) into Ω. This map is then shown to be constant along the orbits of W_s under the action of $(K_s)^n$ (cf. (4.7)), and so defines the promised map f_s of the base space Γ_s into Ω.

For $(c_1,\cdots,c_n)=p\in W_s$, we put $\pi^k(p)=c_1\cdot c_2\cdot\cdots\cdot c_k$, for $k=1,\cdots,n$, and $\pi^0(p)=e$.

DEFINITION 5.2. *$\bar{f}_s(p)$ is the map of $[0,1]$ into M, whose restriction to $[t_i,t_{i+1}]$ equals $\pi^i(p)\cdot s_i$; i.e., for $t\in[t_i,t_{i+1}]$, one has $\bar{f}_s(p)(t)=\pi^i(p)\cdot s_i(t)$.*

We write symbolically

$$\bar{f}_s(p)=\pi^0(p)\cdot s_0+\pi^1(p)\cdot s_1+\cdots+\pi^n(p)\cdot s_n.$$

The map $\bar{f}_s(p)$ is well defined: The value $\bar{f}_s(p)(t)$ has a double definition for $t=t_{i+1}$, $0\leqq i\leqq n-1$, namely $\pi^i(p)\cdot s_i(t_{i+1})$ and $\pi^{i+1}(p)\cdot s_{i+1}(t_{i+1})$. The two values are identical because firstly $s_i(t_{i+1})$ and $s_{i+1}(t_{i+1})$ are identical and secondly $\pi^{i+1}(p)$ differs from $\pi^i(p)$ by the factor c_{i+1} in the stabilizer of $s_{i+1}(t_{i+1})$.

Since K acts by isometries, each $\pi^i(p)\cdot s_i$ is isometric with s_i; it follows easily that the curve $\bar{f}_s(p)$ is parametrized proportionally to arc length. The initial point of $\bar{f}_s(p)$ is R (since $\pi^0(p)\cdot s_0(0)=e\cdot R=R$); the terminal point is $\pi^n(p)\cdot s_n(1)=c_1\cdot\cdots\cdot c_n\cdot s(1)$ and so lies on N because $s(1)$ does. All this implies that the curve $\bar{f}_s(p)$ is a point of $\Omega(M;R,N)$. It can be described as a polygon, consisting of first s_0, then s_1, moved by c_1, then s_2, moved by $c_1\cdot c_2$, etc.

Let $\bar{f}_s\colon W_s \rightarrow \Omega$ be the map which assigns to $p \in W_s$ the element $\bar{f}_s(p)$ of Ω. The continuity of $\bar{f}_s$ is clear. However, $\bar{f}_s$ is in general not 1-1; in fact, each orbit under the action (4.7) of $(K_s)^n$ maps into a single point.

Let $q = (a_1, \cdots, a_n) \in (K_s)^n$. From the definition of the action of $(K_s)^n$ on W_s, one concludes that

$$\pi^i(p \cdot q) = \pi^i(p) \cdot a_i. \tag{5.3}$$

Since $a_i \cdot s = s$, and so $a_i \cdot s_i = s_i$, it follows at once that

$$\bar{f}_s(p \cdot q) = \bar{f}_s(p).$$

This means that the map $\bar{f}_s\colon W_s \rightarrow \Omega$ can be factored through the base space Γ_s under the projection ψ_s, i.e. that there exists a (unique) map $f_s\colon \Gamma_s \rightarrow \Omega$, such that $\bar{f}_s = f_s \circ \psi_s$:

(5.4)
$$\begin{tikzcd} W_s \arrow[d, "\psi_s"'] \arrow[dr, "\bar{f}_s"] & \\ \Gamma_s \arrow[r, dashed, "f_s"'] & \Omega. \end{tikzcd}$$

PROPOSITION 5.5. *f_s is a homeomorphism of Γ_s into Ω.*

Proof. Suppose $p = (c_1, \cdots, c_n)$ and $p' = (c'_1, \cdots, c'_n)$, two points of W_s, have the same $\bar{f}_s$-image, i.e. the relations

$$\pi^i(p) \cdot s_i = \pi^i(p') \cdot s_i \text{ hold.}$$

Since none of the s_i for $1 \leqq i \leqq n$ is degenerate (so that $K_s = K_{s_i}$), it follows that $\pi^i(p)^{-1} \cdot \pi^i(p') = a_i$ belongs to K_s, for $1 \leqq i \leqq n$. This implies easily that $p' = p \cdot q$ with $q = (a_1, \cdots, a_n)$, and Proposition 5.5 is an immediate consequence.

Let $\omega_s \in \Gamma_s$ be the point $\psi_s(e, \cdots, e)$, i.e. the point whose inverse image under ψ_s is the fiber $(K_s)^n$; the f_s-image of ω_s is the geodesic segment s itself. Proposition 5.5 implies as a special case

PROPOSITION 5.5′. *The inverse image under f_s of the point s of Ω is the point ω_s of Γ_s.*

6. Jacobi fields; variational completeness. Our purpose is to formulate sufficient conditions for the cycles Γ_s to generate the homology of Ω. Before we can state our main result in this direction (cf. no. 7), we have to recall some facts concerning Jacobi fields. These vector fields can be defined in the following manner.

A geodesic variation $\{V_\alpha\}$ of a geodesic g in M is a C^∞-map $V\colon \boldsymbol{R}\times I\to M$, where I is an open interval containing 0, such that

(6.1) for each $\alpha\in I$ the map $V_\alpha\colon \boldsymbol{R}\to M$, defined by $V_\alpha(t)=V(t,\alpha)$, is a geodesic,

(6.2) $$V_0=g.$$

DEFINITION 6.3. *The vector field* η *along* g, *defined by* $\eta(t)=\partial V(t,0)/\partial\alpha$, *is called the Jacobi field, or J-field, determined by the geodesic variation* V.

It is well known that the J-fields along g form a vector space, which we shall call J_g, of dimension $2r$ (where $r=\dim M$), and that they can also be characterized as the solutions of the Jacobi differential equations (cf. [16]).

If h is a 1-parameter group in K, then the family $h(\alpha)\cdot g$, $\alpha\in\boldsymbol{R}$ is a geodesic variation of g; this implies that the restriction of any infinitesimal K-motion (cf. Definition 1.6) to g is a J-field along g. From the standard formula for the first variation of arc length, one derives easily that for any infinitesimal K-motion X the inner product $(\dot g(t),\tilde X(g(t)))$ is independent of t.

We indicate now the proof of Proposition 2.2 as promised there. By (1.7), transversality of g at t means the vanishing of $(\dot g(t),\tilde X(g(t)))$ for all $X\in\mathfrak{k}$. By the remark just made, this inner product will vanish for all t, provided it does so for any one particular value t_0.

We shall have to consider all those J-fields along g that vanish at some given parameter value t_0.

DEFINITION 6.4. *For any* $t_0\in\boldsymbol{R}$, $\Lambda_g(t_0)$ *is the subspace of* J_g *consisting of those J-fields that vanish at* t_0;

$$\Lambda_g(t_0)=\{\eta\in J_g\colon \eta(t_0)=0\}.$$

It can be shown that any J-field in $\Lambda_g(t_0)$ can be derived from a variation with fixed point at t_0, i.e., a variation $\{V_\alpha\}$ such that $V(t_0,\alpha)=g(t_0)$ for all $\alpha\in I$. Since a geodesic is determined by its tangent vector at any point, a variation with fixed point at t_0 is equivalent to a curve $Y(\alpha)$ in the tangent space $M_{g(t_0)}$, with $Y(0)=\dot g(t_0)$; in terms of V, we have $Y(\alpha)=\partial V(t_0,\alpha)/\partial t$. The corresponding J-field, derived by differentiation with respect to α, depends only on the vector $\dot Y(0)$. This amounts to a map θ from $M_{g(t_0)}$ (using the customary identification of a vector space with its tangent space at any of its points) into $\Lambda_g(t_0)$; actually, the map is an isomorphism of the two spaces involved. Suppose the variations are further restricted by the requirement that the tangent vectors of the V_α at t_0 lie in a given subspace W of $M_{g(t_0)}$;

then the associated J-fields will form a subspace W' of $\Lambda_{g(t_0)}$, and θ will map W onto W'. We omit the proofs of the various assertions made; they are classical, although usually stated in a different language.

DEFINITION 6.5. *Suppose g is a K-transversal geodesic (cf. no. 2); a J-field is called transversal if it is derived from a geodesic variation $\{V_\alpha\}$ of g in which all V_α are transversal geodesics.*

PROPOSITION 6.6. *If g is a transversal geodesic, then the restriction of any infinitesimal K-motion to g is a transversal J-field.*

This follows at once from the fact that the maps π_k (cf. no. 1) preserve transversality and that therefore each $h(\alpha)\cdot g$ is a transversal geodesic.

DEFINITION 6.7. *Let g be a transversal geodesic, and let t_0 be a real number. We denote by $J_g{}^\pi(t_0)$ the subspace of J_g of those transversal J-fields which at t_0 are tangent to the K-orbit of $g(t_0)$.*

This equals the $J_g{}^N$ of [6], with N the orbit of $g(t_0)$. Remarks similar to those made after 6.4 apply. The dimension of $J_g{}^\pi(t_0)$ is $r=\dim M$ (to obtain $\eta\in J_g{}^\pi(t_0)$, one varies the vector $\dot g(t_0)$ in the r-dimensional manifold of vectors ($\neq 0$) transversal to the orbit of $g(t_0)$).

Let $\tilde X$ be an infinitesimal K-motion, which therefore restricts to a transversal J-field η along the transversal geodesic g. It is clear from (1.7) that η is tangent to the orbit at every point of g, i.e. $\eta\in J_g{}^\pi(t)$ for all t.

The basic property which we require of our group K is laid down in the following definition (cf. [6], p. 261).

DEFINITON 6.8. *The action of K on M is variationally complete if every transversal J-field η, which is tangent to the K-orbits for two different points (parameter values) of the underlying transversal geodesic g (i.e., for which there exist $t_0, t_1\in\mathbf{R}$, $t_0\neq t_1$, such that $\eta\in J_g{}^\pi(t_0)\cap J_g{}^\pi(t_1)$) is induced by K, i.e. is the restriction to g of an infinitesimal K-motion.*

We get an equivalent definition, (6.8′), if instead of requiring tangency at two points, we require tangency at one point and vanishing at another point, i.e. $\eta\in J_g{}^\pi(t_0)\cap\Lambda_g(t_1)$. Clearly, if (6.8) holds, then also (6.8′) holds. We consider the reverse implication: Let (6.8′) hold, and let η be a transversal J-field in $J_g{}^\pi(t_0)\cap J_g{}^\pi(t_1)$. Since $\eta(t_0)$ is tangent to the orbit, there exists an infinitesimal K-motion $\tilde X$, such that $\tilde X(g(t_0))=\eta(t_0)$. Denote by ζ the restriction of $\tilde X$ to g. Then $\eta-\zeta$ is a transversal J-field which vanishes at t_0 and is tangent to the orbit at t_1. By (6.8′), it is therefore induced by K; but then $\eta=(\eta-\zeta)+\zeta$ is also induced by K.

7. The main theorem. For any space X and Abelian group $\boldsymbol{G}$, we denote by $H_r(X;\boldsymbol{G})$ the r-th singular homology group of X with coefficients in $\boldsymbol{G}$; similarly, $H_r(X,A;\boldsymbol{G})$ denotes the relative homology group of X modulo the subset A. We put $H_*(X;\boldsymbol{G})=\sum_r H_r(X;\boldsymbol{G})$. We denote the integers by $\boldsymbol{Z}$ and the integers modulo 2 by $\boldsymbol{Z}_2$. In the case $\boldsymbol{G}=\boldsymbol{Z}$, we write simply $H_*(X)$, etc. If $f\colon X\to Y$ is a map, then f_* is the induced homology map.

Cohomology is indicated by upper indices, $H^r(X;\boldsymbol{G})$, etc. If $\boldsymbol{G}$ is a commutative ring with unit, then $H^*(X;\boldsymbol{G})$ is a graded $\boldsymbol{G}$-algebra (cup product). We write $x(y)$ for the value of a cocycle x on a cycle y.

A fundamental cycle on a manifold, with coefficients in $\boldsymbol{Z}$ or $\boldsymbol{Z}_2$, is the sum of fundamental cycles (i.e. generators of the homology groups in the highest dimension) for the various components of the manifold.

DEFINITION 7.1 (cf. [6], Proposition 6.1). *The defect $\delta(Q)$ of a point Q of M is the difference between the maximum of the dimensions of K-orbits in M and the dimension of the K-orbit of Q.*

Let R be a point with maximal orbit dimension, i.e. with $\delta(R)=0$; it is clear that $\delta(Q)$ can be expressed in terms of stabilizers by

$$\delta(Q)=\dim K_Q-\dim K_R. \tag{7.2}$$

For a geodesic segment $s\colon[a,b]\to M$ we define the defect δ_s by

$$\delta_s=\sum_{a\leqq t<b}\delta(s(t)); \tag{7.3}$$

we shall show later (after Proposition 9.2) that δ_s is finite if $\delta(s(a))=0$.

For each s in the set $S=S(M;R,N)$ (cf. no. 2), we have constructed in no. 4, 5 the manifold Γ_s and the map f_s of Γ_s into Ω. Note that Γ_s is not necessarily connected. For each such s, let $\bar{\gamma}_s$ denote the (unique) fundamental cycle over $\boldsymbol{Z}_2$ of Γ_s. We call S orientable (or better, K-orientable) if all Γ_s are orientable manifolds [i.e., all components of each Γ_s orientable]. In this case, an orientation of S is a function γ which to each $s\in S$ assigns a fundamental cycle γ_s over $\boldsymbol{Z}$ of Γ_s. Only the orientation of the principal component, containing the point $\psi_s(e,\cdots,e)$, will actually matter later. Suppose R lies on an orbit of maximal dimension. It is well known that the stabilizer of any point Q on s, sufficiently close to R, is contained in K_R since s is orthogonal to the orbit of R (existence of a slice [15]). The maximality condition on R implies that the e-components of K_Q and K_R, and therefore also those of K_s and K_R, coincide. We conclude now from (4.5), (7.2), (7.3):

If R has defect 0, then for any $s \in S(M;R,N)$, the relation

(7.4) $\dim \Gamma_s = \delta_s$ *holds.*

Let $\bar{S}_*$, resp. S_*, denote the $\mathbf{Z}_2$-vector space, resp. the free abelian group, with the elements of S as basis, graded by assigning to any s the value δ_s as dimension.

We can now state our first main theorem.

THEOREM I. *Let the action of K on M be variationally complete and let R lie on an orbit of maximal dimension. Then the elements $f_{s*}(\bar{\gamma}_s)$, for $s \in S$, form a basis of (the $\mathbf{Z}_2$-vector space) $H_*(\Omega;\mathbf{Z}_2)$. If S is K-orientable, then $H_*(\Omega;\mathbf{Z})$ is free abelian, with the elements $f_{s*}(\gamma_s)$, for $s \in S$ and γ any orientation of S, as a basis.*

In other words: The assignment $s \rightarrow f_{s*}(\bar{\gamma}_s)$, resp. $s \rightarrow f_{s*}(\gamma_s)$ in the K-orientable case, induces a gradation preserving isomorphism $H_*(\Omega;\mathbf{Z}_2) \approx \bar{S}_*$, resp. $H_*(\Omega;\mathbf{Z}) \approx S_*$ in the K-orientable case.

The two versions of the theorem are equivalent because of (7.4).

The proof of Theorem I, based on the theory of Morse, will be given in the following sections.

We note that Theorem I constitutes an improvement over the results of [6] since it contains a construction of the homology of Ω, whereas Proposition 6.1 of [6], together with the Morse inequalities, essentially gives a majorisation of the Betti numbers of Ω.

Remarks. (a) Consider the case where K reduces to the identity. Each Γ_s is then a point. Variational completeness becomes simply absence of conjugate points. Theorem I says that Ω has no homology in positive dimensions, and that the cardinality of S is equal to the cardinality of the set of arc-components of Ω, i. e. equal to the order of the fundamental group $\pi_1(M)$ of M. If M is simply connected, this means that any two points are connected by exactly one geodesic.

(b) The action of S_1 on S_2, described in no. 2, is easily seen to be variationally complete. The element $f_{s*}(\gamma_s)$, for the s described there, with $R = (1,0,0)$, $N = \{(0,0,1)\}$, is the first Morse cycle, of dimension 1, in $\Omega(S_2)$; an alternative description is as follows: to each point x on the equator of S_2, associate the path consisting of the great circle arc from $(1,0,0)$ to the southpole plus the meridian through x (from $(0,0,-1)$ to $(0,0,1)$); the image of the equator under this map into Ω is the Morse cycle in question. The constructions of Theorem I were motivated by this example.

8. Review of the theory of Morse. We recall some facts and definitions concerning the theory of Morse (cf. [16], [17]).

The values of the length function L on the subset S (made up of the transversal geodesics) of the function space Ω are the stationary values of L. Assume that, for any real l, the collection of elements of S, whose length is $\leqq l$, is finite. The stationary values, in natural order, form then a strictly increasing finite or infinite sequence $\{c_i\}$, $i = 1, 2, \cdots$; if the sequence is infinite, it diverges. If the sequence is finite, one extends it arbitrarily to a strictly increasing, diverging one. To each c_i corresponds then only a finite number of elements of S. Let Ω_i be the subset of Ω determined by $\Omega_i = \{u \in \Omega : L(u) \leqq c_i\}$, the set *up to* level c_i, and let $\Omega_i^- = \{u \in \Omega : L(u) < c_i\}$, the set *strictly below* level c_i; let Ω_0 and Ω_0^- be the empty set.

We define a group E_1 as the direct sum over i of the relative homology groups $H_*(\Omega_i, \Omega_{i-1}; \boldsymbol{G})$, and similarly E_1^- as the direct sum of the groups $H_*(\Omega_i, \Omega_i^-; \boldsymbol{G})$; the notation E_1, E_1^- is used because of the connection with spectral sequences. The following two propositions express Morse's evaluation of the group E_1.

PROPOSITION 8.1. *The inclusions* $(\Omega_i, \Omega_{i-1}) \subset (\Omega_i, \Omega_i^-)$ *induce isomorphisms of* $H_*(\Omega_i, \Omega_{i-1}; \boldsymbol{G})$ *and* $H_*(\Omega_i, \Omega_i^-; \boldsymbol{G})$, *and induce therefore an isomorphism of* E_1 *and* E_1^-.

We sketch briefly how this proposition follows from Morse's work. Put $w_i = \{s \in S : L(s) = c_i\}$, and $\Omega(c) = \{u \in \Omega : L(u) \leqq c\}$ for $c \geqq 0$. The main construction (cf. [17, Satz, p. 66]) consists in finding, for any c with $c_i \leqq c < c_{i+1}$, a deformation D_t, $0 \leqq t \leqq 1$, of the pair $(\Omega(c), \Omega_i^- \cup w_i)$ such that always $D_t(\Omega(c)) \subset \Omega(c)$, $D_t(\Omega_i^- \cup w_i) \subset \Omega_i^- \cup w_i$, and moreover $D_1(\Omega(c)) \subset \Omega_i^- \cup w_i$. It follows that the relative homology groups $H_*(\Omega(c), \Omega_i^- \cup w_i)$ vanish. This implies (by the exact sequence of a triple) that $H_*(\Omega(c), \Omega_i)$ vanishes; one concludes easily that also $H_*(\Omega_{i+1}^-, \Omega_i)$ vanishes, and 8.1 follows. (We note that part of the Theorem on p. 275 in [6] is stated incorrectly; the map mentioned there should be replaced by the two inclusions

$$(\Omega_i^- \cup w_i, \Omega_i^-) \subset (\Omega(l_i), \Omega_i^-) \text{ and } (\Omega(l_i), \Omega(l_{i-1})) \subset (\Omega(l_i), \Omega_i^-).)$$

For non-compact, complete manifolds the argument has to be modified slightly.

To each geodesic segment s in S is assigned an index λ_s (reative to the manifold N): Recall that s is parametrized on $[0, 1]$; call g the underlying geodesic. A value $t_0 \in [0, 1)$ and the point $s(t_0)$ are called focal (for N) if there exists a non-trivial transversal Jacobi field along g that is tangent to N for $t=1$ and vanishes for $t=t_0$, i. e., if the space $J_g{}^{\pi}(1)\cap\Lambda_g(t_0)$ is of positive dimension. The index $\lambda_s(t_0)$ of t_0 is the number of linearly independent such fields: $\lambda_s(t_0)=\dim J_g{}^{\pi}(1)\cap\Lambda_g(t_0)$. It is shown in [16] that each s has only a finite number of focal values.

DEFINITION 8.2. *The index* λ_s (*relative to* N) *of the geodesic segment* s *is given by*

$$\lambda_s=\sum_{0\leqq t<1}\lambda_s(t)=\sum_{0\leqq t<1}\dim J_g{}^{\pi}(1)\cap\Lambda_g(t).$$

The segment s is called non-degenerate (in the sense of Morse) if $\lambda_s(0)=0$, i. e. if 0 is not a focal value. If all $s\in S$ are non-degenerate, then the finiteness assumption, made in the third sentence of this section, is satified. This is an immediate consequence of the implicit function theorem; for another approach cf. [16], Ch. VII, Theorem 11.1.

Assuming s non-degenerate, then there exists, according to Morse, a Euclidean simplex σ_s, of dimension λ_s, and a map $\phi_s\colon\sigma_s\to\Omega$, satisfying the following conditions: (a) the barycenter of σ_s goes into the point s of Ω, (b) the function $L\circ\phi_s$, induced by the length function on Ω, takes its maximum at the barycenter of σ_s, and only there, (c) $L\circ\phi_s$ is of class C^∞ near the barycenter, and the maximum is non-degenerate (i. e. the quadratic terms of the Taylor expansion constitute a negative definite form). Any singular simplex satisfying (a), (b), (c) will be said to be associated to s or "hanging over s" (using an intuitive term motivated by thinking of L, the length, as indicating the "height" of the points of Ω).

Let $\dot\sigma_s$ denote the boundary of σ_s. Then ϕ_s maps the pair $(\sigma_s,\dot\sigma_s)$ into the pair (Ω_i,Ω_i^-), with i determined by $c_i=L(s)$, by condition (b). Recall that the relative homology group $H_r(\sigma_s,\dot\sigma_s;\boldsymbol{G})$ is non-trivial only for $r=\dim\sigma_s=\lambda_s$.

PROPOSITION 8.3. *Assume that all* $s\in S$ *are nondegenerate; choose for each* s *an associated singular simplex* (σ_s,ϕ_s). *Let* ξ_s, *resp.* $\bar\xi_s$, *denote a generator of* $H_{\lambda_s}(\sigma_s,\dot\sigma_s;\boldsymbol{G})$ *for* $\boldsymbol{G}=\boldsymbol{Z}$, *resp.* $\boldsymbol{Z}_2$. *Then, for each* i, *the group* $H_*(\Omega_i,\Omega_i^-)$ *is free abelian, with a basis consisting of the* ϕ_{s*}*-images of the elements* ξ_s, *for all* s *with* $L(s)=c_i$; *similarly, the* ϕ_{s*}*-images of the elements* $\bar\xi_s$, *for* $L(s)=c_i$, *form a basis of the* $\boldsymbol{Z}_2$*-vector space* $H_*(\Omega_i,\Omega_i^-;\boldsymbol{Z}_2)$.

We note that this implies $H_*(\Omega_i,\Omega_i^-;\boldsymbol{G})=0$ if there is no s with $L(s)=c_i$; this will happen, under our convention, for large i, if the number of stationary values is finite.

The simplest situation in which one can deduce the homology of Ω from E_1 is that in which the condition of "completability" holds:

CONDITION 8.4. *For each i and r the map* $j_i\colon H_r(\Omega_i; G) \to H_r(\Omega_i, \Omega_i^-; G)$, *induced by the inclusion of* (Ω_i, Ω_0) *in* (Ω_i, Ω_i^-) *is onto.*

Geometrically this means that every relative cycle of $\Omega_i \bmod \Omega_i^-$, represented by an associated simplex "hanging over" a point s of $\Omega_i - \Omega_i^-$, can be completed "below level $c_i = L(s)$" to an absolute cycle of Ω.

PROPOSITION 8.5. (A) *Suppose all* $s \in S$ *are non-degenerate and the completability condition* (8.4) *holds for* $\boldsymbol{G} = \boldsymbol{Z}$. *For each* $s \in S$, *let* x_s *be an element of* $H_*(\Omega_i)$, *with i determined by* $c_i = L(s)$, *such that* $j_i(x_s) = \phi_{s*}(\xi_s)$. *Let* z_s *be the image of* x_s *in* $H_*(\Omega)$ *under the inclusion* $\Omega_i \subset \Omega$. *Then* $H_*(\Omega)$ *is a free abelian group, and the set* $\{z_s\}$, $s \in S$, *is a basis.*

(B) *A similar statement holds for the case* $\boldsymbol{G} = \boldsymbol{Z}_2$, *with elements* $\bar{x}_s \in H_*(\Omega_i)$, *and with the set* $\{\bar{z}_s\}$, $s \in S$, *forming a base of the* $\boldsymbol{Z}_2$*-vector space* $H_*(\Omega; \boldsymbol{Z}_2)$.

Note that the z_s and $\bar{z}_s$ are completions of the relative cycles $\phi_{s*}(\xi_s)$ and $\phi_{s*}(\bar{\xi}_s)$.

We indicate briefly how Proposition 8.5 follows from (8.1) and (8.3) under condition 8.4, for the case of $\boldsymbol{G} = \boldsymbol{Z}$. From (8.1) and (8.3), one concludes that each $H_*(\Omega_i, \Omega_{i-1})$ is free. From the exactness of the homology sequence of (Ω_i, Ω_{i-1}) and (8.4), one concludes that the sequence

$$0 \to H_*(\Omega_{i-1}) \to H_*(\Omega_i) \to H_*(\Omega_i, \Omega_{i-1}) \to 0$$

is exact. One proves now inductively that each $H_*(\Omega_i)$ is free, and imbedded as direct summand in $H_*(\Omega_{i+1})$ under the inclusion $\Omega_i \subset \Omega_{i+1}$. Since $H_*(\Omega)$ is easily seen to be the direct limit of the $H_*(\Omega_i)$, it follows that it is free abelian. The statement concerning the basis $\{z_s\}$ for $H_*(\Omega)$ is verified by tracing the ξ_s through the construction.

9. Proof of Theorem I. Beginning. We shall show that the hypotheses of Proposition 8.5 are satisfied, if those of Theorem I are.

PROPOSITION 9.1. *Let the point R lie on a K-orbit of maximal dimension and suppose the action of K is variationally complete; then all geodesic segments making up the set* $S = S(M; R, N)$ *are non-degenate in the sense of Morse.*

Proof. Let s be an element of S, carried by the geodesic g. We have to show that the index $\lambda_s(0)$, which equals the dimension of $J_g^\pi(1) \cap \Lambda_g(0)$, vanishes. By the variational completeness assumption 6.8, any J-field in

$J_g{}^\pi(1) \cap \Lambda_g(0)$ is induced by an infinitesimal K-motion (cf. (1.5)) which in turn is derived from a variation of the form $h(\alpha) \cdot g$, where h is a 1-parameter group in K with the property: $h(\alpha) \cdot R = R$ for all α (the variation must leave R fixed, since the J-field vanishes at R). In other words, the elements $h(\alpha)$ are contained in the stabilizer K_R. As in the proof of (7.4), one sees that the e-components of K_g and K_R coincide. This means that the 1-parameter group h above leaves every point of g fixed, and the associated J-field vanishes identically, q. e. d.—The next step is to prove that the completability condition 8.4 is satisfied, and that in fact the K-cycles Γ_s under the maps f_s can be used as completions. The proof is more complicated than that of Proposition 9.1. Let again s be an element of S.

PROPOSITION 9.2. *For any* $t \in [0,1)$, *the inequality* $\dim K_{s(t)} - \dim K_s \leqq \lambda_s(t)$ *holds; if the action of K is variationally complete, then equality obtains.*

Proof. Every X in the Lie algebra $\mathfrak{k}$ produces, through the corresponding infinitesimal K-motion $\tilde{X}$, a transversal Jacobi field; because of (1.7), this field belongs automatically to $J_g{}^\pi(1)$. The field $\tilde{X}$ vanishes at the point $s(t)$ exactly if X belongs to the Lie algebra $\mathfrak{k}_{s(t)}$ of $K_{s(t)}$. This means that there is a map, obviously linear, of $\mathfrak{k}_{s(t)}$ into $J_g{}^\pi(1) \cap \Lambda_g(t)$. The kernel of this map consists of those X whose associated $\tilde{X}$ vanishes identically along s; it is clear that this is just the Lie algebra $\mathfrak{k}_s$ of K_s. The inequality

$$\dim \mathfrak{k}_{s(t)} - \dim \mathfrak{k}_s \leqq \dim J_g{}^\pi(1) \cap \Lambda_g(t)$$

of (9.2) is an immediate consequence. Assume now variational completeness. This means that every J-field in $J_g{}^\pi(1) \cap \Lambda_g(t)$ is induced by an infinitesimal K-motion. The map of $\mathfrak{k}_{s(t)}$ into $J_g{}^\pi(1) \cap \Lambda_g(0)$ introduced above is onto, and the equality of (9.2) follows.

We note that Proposition 9.2 implies the statements about exceptional values made after Definition 4.1 and after (7.3).

PROPOSITION 9.3. *If the action of K is variationally complete, then for every $s \in S$, the dimension of the K-cycle Γ_s equals the index λ_s.*

Proof. By 4.5, we have $\dim \Gamma_s = \sum_i (\dim K_{s(t_i)} - \dim K_s)$, where the sum runs over the exceptional values of s. Proposition 9.3 follows immediately from the Definition 8.2 of λ_s and (9.2). We note that (9.3) and (7.4) imply

(9.4) *If the action of K is variationally complete and $\delta(R) = 0$, then* $\dim \Gamma_s = \lambda_s = \delta_s$ *for every* $s \in S$.

10. A deformation of the K-cycles. Let s be a geodesic of S, and let i be the number of its stationary level: $L(s)=c_i$. In (5.4), we constructed a map $f_s\colon \Gamma_s\to\Omega$, and it is clear from the construction that all polygons making up the image set of f_s have the same length. Hence f_s maps Γ_s into Ω_i.

PROPOSITION 10.1. *Under the hypotheses of Theorem* I, *there is only one geodesic segment in the set* $f_s(\Gamma_s)$, *namely* s *itself; all other elements are geodesic polygons with at least one corner.*

Proof. Since 0 now is not an exceptional value by (9.1), it follows that the interval s_0 on s, introduced in (5.1), is non-degenerate. All elements of $f_s(\Gamma_s)$ are geodesic polygons beginning with s_0. If two geodesic segments have a non-degenerate segment in common, they are identical, q. e. d.

It is possible, and basic for the application of the theory of Morse, to deform f_s in such a way that all $f_s(x)$, except s itself, are replaced by shorter curves, by "cutting across the corners" of the polygons. Actually, a sharper statement has to be made.

PROPOSITION 10.2. *If the segment* s *is non-degenerate in the sense of Morse, then there exists a homotopy* $f_s^u\colon \Gamma_s\to\Omega$, $0\leqq u\leqq 1$, *such that*

(a) $f_s^0=f_s$,

(b) $f_s^u(\omega_s)=s$ *for all* $u\in[0,1]$,

(c) f_s^u *maps* $\Gamma_s-\omega_s$ *into* Ω_i^-, *whenever* $0<u\leqq 1$,

(d) *for any* $u\in(0,1]$, *the induced length function* $L_s^u=L\circ f_s^u$ *on* Γ_s, *which by* (b), (c) *takes it maximum,* $L(s)$, *exactly at* ω_s, *has a non-degenerate critical point at* ω_s.

Assertion (d) means that L_s^u is differentiable near ω_s, and that, in terms of a local coordinate system $\{y_i\}$ at ω_s, the Hessian of L_s^u, i. e. the matrix $(\partial^2 L_s^u/\partial Y_i\partial Y_j\,|_{\omega_s})$, is non-singular; it will then automatically be negative definite, since L_s^u has a maximum at ω_s.

We first define a homotopy $\bar{f}_s^u$ of the map $\bar{f}_s$ of W_s into Ω (cf. no. 5).

Let U be an open neighborhood of s in M, invariant under K and with compact closure; such sets exist. It is known from Riemannian geometry that there is a positive $a=a(U)$ such that any closed sphere V of radius a with center in $\bar{U}$ is geodesically convex (so that any two points of V are joined within V by a unique geodesic segment that varies smoothly with the points and whose length equals the distance of the points). Let ϵ be a number such that

(10.3) $0<\epsilon<a(U)$,

(10.3′) $2\epsilon < L(s_i)$, $i = 0, \cdots, n$, where the s_i are the intervals on s, defined by the exceptional points (cf. (5.1)).

For any $u \in [0,1]$, we let $s_i{}^u$ be the following restrictions of s, with $u' = u \cdot \epsilon / L(s)$:

$$
\begin{aligned}
&s_0{}^u = s \mid [0, t_1 - u'],\\
(10.4)\qquad &s_i{}^u = s \mid [t_i + u', t_{i+1} - u'], \text{ for } i = 1, \cdots, n-1,\\
&s_n{}^u = s \mid [t_n + u', 1].
\end{aligned}
$$

Because of (10.3′), the indicated intervals of $[0,1]$ are all non-degenerate:

$$2u' \leqq 2\epsilon / L(s) < L(s_i)/L(s) = t_{i+1} - t_i.$$

We denote by $\alpha_i(u)$, resp. $\beta_i(u)$, the initial, resp. terminal point of the segment $s_i{}^u$.

Let $p = (c_1, \cdots, c_n)$ be any point of W_s. Using the notation introduced in no. 5, we let $r_i{}^u(p)$ be the unique shortest geodesic segment from $\pi^i(p) \cdot \beta_i(u)$ to $\pi^{i+1}(p) \cdot \alpha_{i+1}(u)$, parametrized from $t_{i+1} - u'$ to $t_{i+1} + u'$, for $i = 0, \cdots, n-1$.

The existence of $r_i{}^u(p)$ comes from the fact that the two points which it is supposed to connect lie with the ϵ-sphere around the point $\pi^i(p) \cdot s_i(t_{i+1}) \in U$, and (10.3) applies.

DEFINITION 10.5. *$\bar{f}_s{}^u(p)$ is the geodesic polygon, parametrized on $[0,1]$ proportionally to arc length, made up of the segments*

$$\pi^0(p) \cdot s_0{}^u, \quad r_0{}^u(p), \quad \pi^1(p) \cdot s_1{}^u, \quad r_1{}^u(p), \cdots, \quad r_{n-1}{}^u(p), \quad \pi^n(p) \cdot s_n{}^u.$$

As indicated before, each $\bar{f}_s{}^u(p)$ is a geodesic polygon in Ω (i.e. beginning at R, and ending transversally on N), obtained from $\bar{f}_s(p)$ by "cutting across the corners." The construction is pictured in fig. 1. It follows from local minimum properties of geodesics in convex spheres that $\bar{f}_s{}^u(p)$, for $u > 0$, is actually shorter than $\bar{f}_s(p)$, provided there is at least one corner on $\bar{f}_s(p)$.

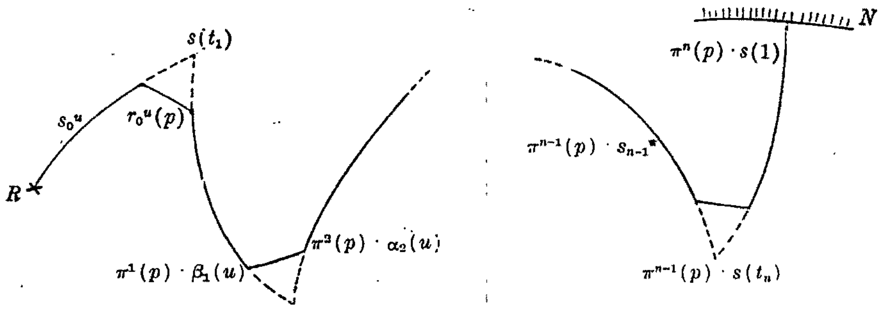

$s(t_1)$
$s_0{}^u$
$r_0{}^u(p)$
R
$\pi^1(p) \cdot \beta_1(u)$
$\pi^2(p) \cdot \alpha_2(u)$
N
$\pi^n(p) \cdot s(1)$
$\pi^{n-1}(p) \cdot s_{n-1}$
$\pi^{n-1}(p) \cdot s(t_n)$

Figure 1.

11. The critical point on Γ_s. It is clear that with the choice of ϵ in (10.3), (10.3′), the point $\bar{f}_s{}^u(p)$ of Ω depends continuously on the pair (p,u). Since $\bar{f}_s{}^u(p)$ is derived from the polygon $\bar{f}_s(p)$ by a geometrical construction, it follows at once that two points p, p' of W_s which are equivalent under the action 4.6 of $(K_s)^n$ on W_s, will give rise to the same modified polygon; i.e. $p' = p \cdot q$ implies $\bar{f}_s{}^u(p') = \bar{f}_s{}^u(p)$. This means that the map $\bar{f}_s{}^u$ of W_s into Ω can be factored through Γ_s, with an induced map $f_s{}^u \colon \Gamma_s \to \Omega$. Clearly $f_s{}^u$ is a homotopy with properties (a), (b) of Proposition 10.2. The induced length function $L_s{}^u$ is clearly constant for $u = 0$. Since 0 is not exceptional for s, Proposition 10.1 applies. By the last remark of no. 10, the function $L_s{}^u$, for $u > 0$, will take a value less than $L(s)$ at every point x of Γ_s, different from ω_s; this proves (10.2 (c)).

The proof of (10.2 (d)) is more complicated. We note first that each $L_s{}^u$ is of class C^∞, since all the points involved in the construction of the geodesic polygons are C^∞-functions of the parameters occurring. We prove (d) in the following equivalent form.

PROPOSITION 11.1. *Let s be non-degenerate in the sense of Morse [and suppose* $\dim \Gamma_s > 0$ *to rule out a trivial case]; let x be a C^∞-curve in Γ_s, defined on some interval $(-a,a)$ with $x(0) = \omega_s$, and $\dot{x}(0) \neq 0$; put $F = L_s{}^u \circ x$ with any u in* $(0,1]$; *then the second derivative of F at the origin 0 is negative:* $F''(0) < 0$.

It is clear from what has been proved already that $F(0) = L(s)$ and $F'(0) = 0$, since F has a maximum at 0. For the proof of (11.1), we take a vector Y at $(e,\cdots,e)$ in W_s that projects into $\dot{x}(0)$ under the map $\psi_s \colon W_s \to \Gamma_s$, and let y be a curve in W_s, through $(e,\cdots,e)$ with $\dot{y}(0) = Y$, that projects into x, so that $\psi_s(y(v)) = x(v)$. Both Y and y exist since ψ_s is a fiber map. We have then $F(v) = L \circ \bar{f}_s{}^u(y(v))$, since $f_s{}^u$ is induced by $\bar{f}_s{}^u$.

Suppose first that y is of the form $y(v) = (e,\cdots,e, y_{i_0}(v), e, \cdots, e)$, i.e. that it has only one non-constant component. This means that the geodesic polygon $\bar{f}_s(y(v))$, for any v, has exactly one corner at parameter value t_{i_0}.

Let $\phi(v)$ stand for the length of the geodesic segment from $s(t_{i_0} - u')$ $= \beta_{i_0-1}(u)$ to $y_{i_0}(v) \cdot s(t_{i_0} + u') = y_{i_0}(v) \cdot \alpha_{i_0}(u)$, which cuts across the corner of $\bar{f}_s(y(v))$ to form $\bar{f}_s{}^u(y(v))$. We clearly have $F(v) = L(s) - 2u' \cdot \epsilon + \phi(v)$. The vector Y is not in the kernel of ψ_s, and is therefore not tangent to the submanifold $\psi_s{}^{-1}(\omega_s) = (K_s)^n$ of W_s. This means that $\dot{y}_{i_0}(0)$ is not tangent to K_s. Since $t_{i_0}+u'$ is not exceptional for s, this implies that the curve defined by $z(v)=y_{i_0}(v)\cdot s(t_{i_0}+u')$ has a non-zero tangent vector at $v=0$. The assertion $\phi''(0)<0$ reduces therefore to the following: Let a, b be the end points of a geodesic segment of length 2ϵ, whose midpoint c lies in $\bar{U}$; let $b(v)$ be a C^∞-curve such that (1) $b(0)=b$, (2) $b(v)$ lies on the ϵ-sphere around c, (3) $\dot{b}(0)\neq 0$; then for $d(v)$ defined as the distance from a to $b(v)$, the relation $d''(0)<0$ holds. This property of geodesic spheres (elementary for Euclidean space) is well known to hold, provided $a(U)$ is chosen sufficinetly small.

We consider now an arbitrary curve y, without the restriction made above. The vector $Y=(\dot{y}_1(0),\cdots,\dot{y}_n(0))$ is again not tangent to $(K_s)^n$ at $(e,\cdots,e)$, so that at least one of the $\dot{y}_i(0)$, say $\dot{y}_{i_0}$, is not tangent to the submanifold K_s of K_{i_0} at e. We put $y_0(v)=(e,\cdots,e,y_{i_0}(v),e,\cdots,e)$, and compare $\bar{f}_s{}^u(y(v))$ with $\bar{f}_s{}^u(y_0(v))$. The shortening process at the corner at t_{i_0} reduces both curves by the same amount from the original value $L(s)$. The latter curve has only this one corner, the former may have several corners; it follows that the former is not longer than the latter. Putting $F_0(v)=L\circ\bar{f}_s{}^u(y_0(v))$, we have therefore $F(v)\leqq F_0(v)$. The reasoning above applies to F_0, since y_0 has only one non-constant component. We have therefore $F_0''(0)<0$. In addition, we have $F(0)=F_0(0)=L(s)$, and $F'(0)=F_0'(0)=0$, as noted before. It is elementary that then $F''(0)\leqq F_0''(0)$, and so finally $F''(0)<0$. Propositions 11.1 and 10.2 are proved.

12. Proof of Theorem I completed. For each $s\in S$, choose a Euclidean simplex σ_s, with $\dim\sigma_s=\dim\Gamma_s$, and a regular C^∞-homeomorphism ρ_s of σ_s into Γ_s such that ρ_s sends the barycenter of σ_s into ω_s. Define $\phi_s\colon\sigma_s\to\Omega$ by $\phi_s=f_s{}^u\circ\rho_s$ for some positive u. By (9.3) and (10.2), the singular simplex (σ_s,ϕ_s) is associated to s in the sense of no. 8. Put $g_s=f_s{}^u$, considered as a map into Ω_i.

$$\begin{tikzcd}
 & \Gamma_s \arrow[r, "g_s"] \arrow[d, "j_s"'] & \Omega_i \arrow[d, "j_i"] \\
(\sigma_s, \dot{\sigma}_s) \arrow[r, "\rho_s"] & (\Gamma_s, \Gamma_s - \{\omega_s\}) \arrow[r, "g_s"] & (\Omega_i, \Omega_i^-)
\end{tikzcd}$$

We consider the commutative diagram above, where the vertical maps are simply inclusion maps. Let first $\mathbf{Z}_2$ be taken as coefficient group. It is clear by excision that the j_s-image of the fundamental cycle of Γ_s equals the ρ_s-image of the fundamental cycle of $(\sigma_s,\dot{\sigma}_s)$; with the notations of Theorem I and

(8.3) we have $j_{s*}(\bar{\gamma}_s) = \rho_{s*}(\bar{\xi}_s)$. Applying g_{s*} (with $g_{s*} \circ \rho_{s*} = \phi_{s*}$) and using the commutativity of the diagram, one concludes that $\phi_{s*}(\bar{\xi}_s) = j_{i*}(g_{s*}(\bar{\gamma}_s))$, so that $\phi_{s*}(\bar{\xi}_s)$ is contained in $j_{i*}(H_{\lambda_s}(\Omega_i;\mathbf{Z}_2))$. Since this holds for every s, it follows now from (8.3) that the completability condition 8.4 holds for $G = Z_2$.

For the case of $\mathbf{G} = \mathbf{Z}$, assume that S is K-orientable, and let γ be an orientation of S, as defined prior to Theorem I. Again it is clear, by excision, that for a suitably chosen generator ξ_s of $H_{\lambda_s}(\sigma_s, \dot{\sigma}_s)$ the relation $j_{s*}(\gamma_s) = \rho_{s*}(\xi_s)$ holds. The rest of the argument goes as before, and shows that 8.4 holds.

Non-degeneracy of all s has been proved in (9.1) already. With non-degeneracy and completability following from the hypotheses of Theorem I, we can now apply Proposition 8.5 with $\bar{x}_s = g_{s*}(\bar{\gamma}_s)$, or, in the K-orientable case, with $x_s = g_s(\gamma_s)$. Theorem I follows directly if we remark that the image of $g_{s*}(\bar{\gamma}_s)$ under the inclusion $\Omega_i \subset \Omega$ is $f_{s*}{}^u(\bar{\gamma}_s)$, and that $f_{s*}{}^u$ is identical with f_{s*}, by the homotopy axiom; similarly for γ_s.

Chapter II. Variational Completeness in Symmetric Spaces.

1. Action of $K \times K$ and of K.

Let G be a compact connected Lie group, and let K be a closed connected subgroup, which then itself is also a Lie group. The direct product $K \times K$ acts from the left on G under the definition

$$(a, b) \cdot c = a \cdot c \cdot b^{-1} \tag{1.1}$$

with $a, b \in K$, $c \in G$; this is an action in the sense of Chapter I, no. 1. We introduce in G a Riemannian metric invariant under left and right translations. It is well known that such metrics exist, and that the geodesics in such a metric are the 1-parameter subgroups and their cosets. In general, we shall follow the notation of [6]. But we write $a \cdot X$ or aX instead $l_a(X)$ for the left translate of the vector X by the element a of G. The adjoint action of G on its Lie algebra $\mathfrak{g}$ is then given by $Ada \cdot x = a \cdot X \cdot a^{-1}$. For the Lie product [,] and the invariant inner product or Killing form (,) in $\mathfrak{g}$ we have then the usual relations:

(1.2)

(a) $\mathrm{Ad}a \cdot [X, Y] = [\mathrm{Ad}a \cdot X, \mathrm{Ad}a \cdot X]$,

(b) $(X, Y) = (\mathrm{Ad}a \cdot X, \mathrm{Ad}a \cdot X)$,

(c) $([X, Y], Z) + (Y, [X, Z]) = 0$,

(d) $d\,\mathrm{Ad}e^{tY} \cdot X/dt\,|_{t=0} = [Y, X] = \mathrm{ad}Y \cdot X$.

As usual, G/K denotes the homogeneous space formed by the left cosets xK, $x \in G$, under the decomposition topology, with the induced C^∞-manifold structure; the group G acts on the left on G/K by $y \cdot (xK) = (yx)K$. Let p denote the natural map of G on G/K. The Riemannian metric of G induces a Riemannian metric on G/K, invariant under the action of G: If X' is a vector at the point $x' \in G/K$, let X be a vector at any point x in $p^{-1}(x')$, orthogonal to the manifold xK and with $\dot{p}(X) = X'$; define the norm $|X'|$ of X' to be equal to the norm $|X|$ of X; the definition is independent of the choice of x involved. In particular, let $\mathfrak{p}$ denote the subspace of the Lie algebra $\mathfrak{g}$ orthogonal to the Lie algebra $\mathfrak{k}$; then $\dot{p}$ gives an isometry of $\mathfrak{p}$ with the tangent space of G/K at $p(e) = e'$. The group K acts on G/K, as subgroup of G. Since K is the stability group of e', it acts on the tangent space $(G/K)_{e'}$. It also acts on $\mathfrak{g}$ by the adjoint transformations Adk. The subspaces $\mathfrak{k}$ and $\mathfrak{p}$ of $\mathfrak{g}$ are invariant under AdK, and the action of K on $\mathfrak{p}$ so defined is equivalent, via the map $\dot{p}$, to the action of K on $(G/K)_{e'}$.

2. Symmetric spaces and variational completeness. We recall E. Cartan's concept of symmetric space [9].

DEFINITION 2.1. *The pair* (G,K) *is called a symmetric pair, if there exists an involution* $*$ *(i.e. automorphism of order two), of* G, *written* $x \to x^*$, *such that* K *is the e-component of the fixed group of the involution (i.e. of the group* $\{x : x^* = x\}$*).*

If (G,K) is a symmetric pair, then G/K is a symmetric space; actually, one can divide G by any closed subgroup of G between K and the fixed group of the involution.

In Chapter I, (8.4), we have defined variational completeness which forms the hypothesis of Theorem I. The following theorem provides cases were this hypothesis holds.

THEOREM II. *Let* (G,K) *be a symmetric pair; then the action of* $K \times K$ *on* G, *the action of* K *on* G/K *and the action of* K *on* $\mathfrak{p}$, *as defined in no. 1, are variationally complete.*

The proof of this theorem is a generalization of that of Proposition 7.1 in [6].

We begin with the action of $K \times K$ on G. Theorem II, for this case, takes the form of Proposition 2.2 below; note that the role of K in Chapter I is now taken by $K \times K$. (For the definitions of transversal geodesic, transversal Jacobi field and infinitesimal $K \times K$-motion see Chapter I, (2.1), (8.2) and no. 1.)

PROPOSITION 2.2. *Let g be a $K \times K$-transversal geodesic of G; let η be a transversal Jacobi field along g that vanishes for $t=0$ and is tangent to the $K \times K$-orbit of $g(1)$ for $t=1$; then η is induced by an infinitesimal $K \times K$-motion.*

For the proof, we shall describe, in Lemma 4.1, the space of all transversal J-fields vanishing for $t=0$; in Lemma 5.1, we describe the space of all infinitesimal $K \times K$-motions; Proposition 2.2 will then follow from a comparison of the two spaces.

3. **Tangent and transversal space of an orbit.** Basic for the proof are the following relations in the Lie algebra $\mathfrak{g}$ of G, which are well known to be equivalent to the existence (locally) of the involution which defines our symmetric pair (G,K):

$$[\mathfrak{k},\mathfrak{k}] \subset \mathfrak{k}; \quad [\mathfrak{k},\mathfrak{p}] \subset \mathfrak{p}; \quad [\mathfrak{p},\mathfrak{p}] \subset \mathfrak{k}. \tag{3.1}$$

We also recall

$$\mathfrak{p} = \mathfrak{k}^{\perp} \text{ (orthogonal complement in } \mathfrak{g}). \tag{3.2}$$

Next we describe the tangent space of an orbit and its orthogonal complement.

DEFINITION 3.3. *For any $a \in G$, we put*

$$\mathfrak{k}^a = \mathfrak{k} + \mathrm{Ad}a^{-1}\cdot\mathfrak{k}; \quad \mathfrak{k}_a = \mathfrak{k} \cap \mathrm{Ad}a^{-1}\cdot\mathfrak{k}$$
$$\mathfrak{p}_a = \mathfrak{p} \cap \mathrm{Ad}a^{-1}\cdot\mathfrak{p}.$$

The relations (3.1) imply similar relations for the spaces defined in (3.3); we give the ones that we shall need later.

$$[\mathfrak{k}_a,\mathfrak{p}_a] \subset \mathfrak{p}_a; \quad [\mathfrak{p}_a,\mathfrak{p}_a] \subset \mathfrak{k}_a; \tag{3.4}$$

$$\mathfrak{p}_a = (\mathfrak{k}^a)^{\perp}. \tag{3.5}$$

(3.4) follows easily from (3.1) and the fact that $\mathrm{Ad}a^{-1}$ is an automorphism of $\mathfrak{g}$. Similarly, (3.5) follows from (3.2) and the fact that $\mathrm{Ad}a^{-1}$ is an isometry of $\mathfrak{g}$.

PROPOSITION 3.6. *The spaces $\mathfrak{k}^a$ and $\mathfrak{p}_a$ are the left translates, under a^{-1}, of the tangent space and the transversal space to the orbit $K\cdot a\cdot K$ at the point a.*

Proof. The tangent space to $K\cdot a\cdot K$ at a is clearly $\mathfrak{k}\cdot a + a\cdot\mathfrak{k}$. Applying

a^{-1} on the left, one gets $\mathfrak{k}^a$. The assertion for $\mathfrak{p}_a$ follows from (3.5) and the isometric character of left translation.

The space $\mathfrak{p}_a$ admits a decomposition relative to any of its elements, which we derive now.

DEFINITION 3.7. *For any* $X \in \mathfrak{g}$, *the centralizer* $\mathfrak{g}_X$ (*a subalgebra of* $\mathfrak{g}$) *consists of the elements* $Z \in \mathfrak{g}$ *with* $[X, Z] = 0$.

LEMMA 3.8. *For any* $X \in \mathfrak{p}_a$, *the space* $\mathfrak{p}_a$ *admits the orthogonal direct sum decomposition*

$$\mathfrak{p}_a = \operatorname{ad}X(\mathfrak{k}_a) \oplus (\mathfrak{p}_a \cap \mathfrak{g}_X).$$

Proof. By (3.4), $\operatorname{ad}X(\mathfrak{k}_a)$ is a subspace of $\mathfrak{p}_a$. Take Z in $\mathfrak{p}_a$, orthogonal to this subspace. Then, for any $Y \in \mathfrak{k}_a$, we have $0 = ([X, Y], Z) = -(Y, [X, Z])$. Since $[X, Z]$ belongs to $\mathfrak{k}_a$ by (3.4) and since Y is arbitrary in $\mathfrak{k}_a$, we have $[X, Z] = 0$, q. e. d.

4. Transversal Jacobi fields. Let now g be a transversal geodesic. We put $g(0) = a$; then g is of the form $a \cdot e^{tX}$, where e^{tX} is the 1-parameter group with initial vector X. By (3.6), the vector X belongs to $\mathfrak{p}_a$.

LEMMA 4.1. *Any transversal Jacobi field* η *along* g *with* $\eta(0) = 0$ *can be written as*

$$\eta(t) = a \cdot e^{tX} \cdot (\operatorname{Ad}e^{-tX} \cdot Y - Y + tZ) \text{ with } Y \in \mathfrak{k}_a, Z \in \mathfrak{p}_a \cap \mathfrak{g}_X.$$

Proof. There are two obvious ways of varying g, with $g(0)$ fixed: conjugation of e^{tX} by elements y of G and multiplication of e^{tX} by e^{tZ} with any Z that commutes with X. To keep the geodesics transversal, we restrict y to $K \cap a^{-1} \cdot K \cdot a$ and Z to $\mathfrak{p}_a$. We shall show that with these two processes, one can produce all transversal variations with $g(0)$ fixed, and the associated J-fields are of the form given in 4.1.

Let then Y be any element of $\mathfrak{k}_a$, and Z any element of $\mathfrak{p}_a \cap \mathfrak{g}_X$. We consider the geodesic $g_{Y,Z}$, given by $a \cdot e^{Y} \cdot e^{t(X+Z)} \cdot e^{-Y}$, with $g_{Y,Z}(0) = a$, and with initial tangent vector $a \cdot \operatorname{Ad}e^{Y} \cdot (X + Z)$. Since $X \in \mathfrak{p}_a$, and $e^{Y} \in K \cap a \cdot K \cdot a^{-1}$ (because of $Y \in \mathfrak{k} \cap \operatorname{Ad}a^{-1} \cdot \mathfrak{k}$) this vector belongs to $a \cdot \mathfrak{p}_a$, and $g_{Y,Z}$ is transversal. Assigning $a \cdot \operatorname{Ad}e^{Y} \cdot (X + Z)$ to the pair (Y, Z) constitutes a map ϕ of $\mathfrak{k}_a \oplus (\mathfrak{p}_a \cap \mathfrak{g}_X)$ into $a \cdot \mathfrak{p}_a$, with $\phi(0,0) = a \cdot X$. Using (1.2(d)), one derives that the differential ϕ_0 at $(0,0)$ maps the pair (Y, Z) into $a \cdot [Y, X] + a \cdot Z$ (we have made use of the customary identification for tangent spaces to vector spaces).

Lemma 3.8 implies that ϕ_0 is a map onto $a \cdot \mathfrak{p}_a$. From the remarks on

J-fields in Chapter I, no. 6, taking $a \cdot \mathfrak{p}_a$ as the space W there, one concludes now that the map which to the vector (Y, Z) assigns the J-field of the variation $a \cdot e^{aY} \cdot e^{t(X+aZ)} e^{-aY}$ is a map of $\mathfrak{k}_a \oplus (\mathfrak{p}_a \cap \mathfrak{g}_X)$ onto the space of transversal J-fields vanishing for $t = 0$. One verifies by straight forward differentiating (using $[X, Z] = 0$) that this J-field is of the type described in (4.1), and so (4.1) is proved.

5. The infinitesimal motions. We first prove

LEMMA 5.1. *The infinitesimal* $K \times K$*-motions, which vanish at* a*, restrict along* g *to the vector fields of the form* $a \cdot e^{tX} \cdot (\mathrm{Ad} e^{-tX} \cdot V - V)$ *with* $V \in \mathfrak{k}_a$.

Proof. All 1-parameter $K \times K$-motions are clearly of the form $y \to e^{aU} \cdot y \cdot e^{-aV}$, with $U, V \in \mathfrak{k}$. The corresponding infinitesimal motion assigns to y the vector $U \cdot y - y \cdot V$. Such a field will vanish at a, if $U \cdot a - a \cdot V = 0$, i.e., if $U = \mathrm{Ad} a \cdot V$. In other words, the infinitesimal motions that vanish at a are of the form $(\mathrm{Ad} a \cdot V) y - y \cdot V$, with $V \in \mathfrak{k}$ and $\mathrm{Ad} a \cdot V \in \mathfrak{k}$, i.e with $V \in \mathfrak{k}_a$. For $y = a \cdot e^{tX}$, along g, this becomes $a \cdot e^{tX} \cdot (\mathrm{Ad} e^{-tX} \cdot V - V)$, q.e.d.

We come now to the proof of Proposition 2.2. Let η be as described there, and let Y, Z be the vectors associated with η by (4.1). The assumption that $\eta(1)$ is tangent to the orbit of $b = a \cdot e^X$ at b means, by (3.6),

$$b^{-1} \cdot \eta(1) = \mathrm{Ad} e^{-X} \cdot Y - Y + Z \in \mathfrak{k}^b. \tag{5.2}$$

Any vector B in $\mathfrak{k}^b$ can be written as $B_1 + B_2$ with $B_1 \in \mathfrak{k}$ and $B_2 \in \mathrm{Ad} b^{-1} \cdot \mathfrak{k}$; we can write B_2 as $\mathrm{Ad} e^{-X} \cdot B_2'$ with $B_2' \in \mathrm{Ad} a^{-1} \cdot \mathfrak{k}$, since $b = a \cdot e^X$. By (3.5), Z is orthogonal to $\mathfrak{k}^a$, so that the inner products (Z, B_1) and (Z, B_2') vanish. We have $\mathrm{Ad} e^X \cdot Z = Z$, since $[X, Z] = 0$. It follows that

$$(Z, B_2) = (\mathrm{Ad} e^X \cdot Z, \mathrm{Ad} e^X \cdot B_2) = (Z, B_2') = 0.$$

This means that $(Z, B) = 0$ and Z is orthogonal to $\mathfrak{k}^b$. From (5.2), we have then $0 = (\mathrm{Ad} e^{-X} \cdot Y - Y + Z, Z) = (\mathrm{Ad} e^{-X} \cdot Y, Z) - (Y, Z) + (Z, Z)$. Since $(\mathrm{Ad} e^{-X} \cdot Y, Z) = (Y, Z)$, we conclude $(Z, Z) = 0$, and so $Z = 0$. But then η is given by $a \cdot e^{tX} \cdot (\mathrm{Ad} e^{-tX} \cdot Y - Y)$, and this is, by (5.1), an infinitesimal motion, since $Y \in \mathfrak{k}_a$.

6. *K* operating on *G/K*. We consider now Theorem II for the action of K on G/K. We will reduce this case, with the help of the projection $p: G \to G/K$, to the previous case of $K \times K$ acting on G. It is well known and easily proved that for the Riemannian metric in G/K, as defined in no. 1, the geodesics in G/K are exactly the projections of those geodesics in G that are orthogonal to the left cosets of K (i. e. to the geodesics which are transversal with respect to the action of K on G, defined by multiplying on the right). For any $a \in G$, the projection of the $K \times K$-orbit $K \cdot a \cdot K$ is the K-orbit $K \cdot a'$, with $a' = p(a)$. The space $a \cdot \mathfrak{p}_a$, the orthogonal complement of the tangent space to $K \cdot a \cdot K$ at a in the tangent space to G at a, is mapped by $\dot{p}$ isometrically onto the orthogonal complement of the tangent space at a' of the orbit $K \cdot a'$. It follows that the $K \times K$-transversal geodesics at a map onto the K-transversal geodesics at a' (in a 1-1 way), and that for any such geodesic at a, the space of transversal Jacobi fields that vanish at a maps onto the space of transversal J-fields along the projected geodesic that vanish at a'; moreover, any such J-field is tangent to the $K \times K$-orbit at a point b, if and only if the projected J-field is tangent to the K-orbit at $b' = p(b)$. In other words, p establishes an isomorphism between $\Lambda_g(0) \cap J_g{}^{\pi}(1)$ and $\Lambda_{g'}(0) \cap J_{g'}{}^{\pi}(1)$ for any transversal geodesic g in G and its projection g' in G/K. Finally, the projection is equivariant with respect to the natural map of $K \times K$ onto its first factor; i. e. $p((k_1, k_2) \cdot a) = k_1 \cdot p(a)$. It follows easily that any infinitesimal $K \times K$-motion along g that vanishes at a projects into an infinitesimal K-motion along g' that vanishes at a'. Since all elements in $\Lambda_g(0) \cap J_g{}^{\pi}(1)$ are induced by $K \times K$, it follows now that all elements in $\Lambda_{g'}(0) \cap J_{g'}{}^{\pi}(1)$ are induced by K, q. e. d.

7. The infinitesimal case. We come to the adjoint action of K on $\mathfrak{p}$, the infinitesimal analogue of the case just treated. We give a proof analogous to that of Proposition 2.2; another possible approach consists in comparing $\mathfrak{p}$ with a small K-invariant neighborhood of e' in G/K. Let A be any point in $\mathfrak{p}$.

PROPOSITION 7.1. *The tangent space to the orbit of A under the adjoint action of K is* $\operatorname{ad}A(\mathfrak{k})$.

This follows from the relation (1.2(d)).

DEFINITION 7.2. $\mathfrak{k}_A = \mathfrak{k} \cap \mathfrak{g}_A$; $\mathfrak{p}_A = \mathfrak{p} \cap \mathfrak{g}_A$ (*here* $\mathfrak{g}_A$ *is the centralizer of* A).

We have the relations:

$$(7.3) \qquad [\mathfrak{k}_A, \mathfrak{p}_A] \subset \mathfrak{p}_A; \quad [\mathfrak{p}_A, \mathfrak{p}_A] \subset \mathfrak{k}_A;$$

$$(7.4) \qquad \mathfrak{p}_A = \operatorname{ad}A(\mathfrak{k})^{\perp} \text{ (orthogonal complement in } \mathfrak{p}).$$

For the proof of (7.3), we use (3.1) and note that by the Jacobi identity, the left sides are contained in $\mathfrak{g}_A$. To prove (7.3), take $P \in \mathfrak{p}$ and $Q \in \mathfrak{k}$. The relation $(P, [A, Q]) = -([A, P], Q)$ together with $[A, P] \in \mathfrak{k}$ (by (3.1)) implies the stated result. Note that $A \in \mathfrak{p}_A$.

Recall that the geodesics in $\mathfrak{p}$ are simply the straight lines. Let X by any element of $\mathfrak{p}_A$ and define the geodesic g by $g(t) = A + tX$; with X varying through $\mathfrak{p}_A$, this represents all the K-transversal geodesics starting at A.

LEMMA 7.5. $\mathfrak{p}_A = \mathrm{ad}X(\mathfrak{k}_A) \oplus (\mathfrak{p}_A \cap \mathfrak{g}_X)$ (*orthogonal decomposition*). The proof is analogous to that of (3.8) with (7.3), (7.4) replacing (3.4), (3.5).

LEMMA 7.6. *Any transversal J-field* η *along* g *with* $\eta(0) = 0$ *can be written as* $\eta(t) = t(E_1 + E_2)$ *with* $E_1 \in \mathrm{ad}X(\mathfrak{k}_A)$, $E_2 \in \mathfrak{p}_A \cap \mathfrak{g}_X$.

Proof. The transversal geodesics are the straight lines of the form $A + tC$, with $C \in \mathfrak{p}_A$, by 7.4. For the study of transversal Jacobi fields vanishing at A, it is clearly sufficient to consider linear variations, i.e. families $\{V_\alpha\}$ with $V_\alpha(t) = A + t\cdot(X + \alpha C)$ for $C \in \mathfrak{p}_A$. The Jacobi field of such a variation is given by tC. Splitting C according to Lemma 7.5, we get Lemma 7.6.

LEMMA 7.7. *The infinitesimal K-motions along* g, *vanishing at* A, *are exactly the fields of the form* $t[Y, X]$ *with* $Y \in \mathfrak{k}_A$.

Proof. The infinitesimal K-motion in $\mathfrak{p}$, determined by the 1-parameter group $\mathrm{Ad}e^{\alpha Y}$, assigns to the point S of $\mathfrak{p}$ the vector $[Y, S]$. Such a field vanishes at A exactly if $Y \in \mathfrak{k}_A$, and the field along g, i.e. for $S = A + tX$, is then $t[Y, X]$.

We prove now that variational completeness holds.

PROPOSITION 7.8. *Let* η *be a transversal Jacobi field along* g *with* $\eta(0) = 0$ *that is tangent to the K-orbit at* $B = A + X$ (*i.e., for* $t = 1$); *then* η *is induced by an infinitesimal K-motion.*

Decompose $\eta(t)$ into $t[X, Y] + tZ$ with $Y \in \mathfrak{k}_A$, $Z \in \mathfrak{p}_A \cap \mathfrak{g}_X$ by Lemma 7.6. To say that $\eta(1)$ is tangent to the orbit is to say that $[X, Y] + Z \in \mathrm{ad}(A + X)(\mathfrak{k})$, by (7.1). We have $([X, Y], Z) = -(Y, [X, Z]) = 0$ because of $[X, Z] = 0$. Take any $D \in \mathfrak{k}$ and form $([A + X, D], Z)$. This equals $-(D, [A, Z]) - (D, [X, Z])$. Since $[A, Z] = [X, Z] = 0$, we conclude that Z is orthogonal to $\mathrm{ad}(A + X)(\mathfrak{k})$. It follows now that $(Z, Z) = 0$, and so $Z = 0$. The proof of Theorem II is complete.

8. G as symmetric space. A well known case of symmetric pairs is obtained by starting with any compact connected Lie group G, forming $G \times G$, and defining an involution in $G \times G$ by $(x,y)^* = (y,x)$. The fixed group is then the diagonal Δ, isomorphic to G under $x \to (x,x)$. The quotient space $(G \times G)/\Delta$ can be identified with G through the map $(x,y) \to x \cdot y^{-1}$. The action of Δ on $(G \times G)/\Delta$ goes over into the action of G on itself by inner automorphisms. Similarly, the adjoint action of Δ on the tangent space of $(G \times G)/\Delta$ at the image of (e,e) (or on the subspace $\{(X, -X) : X \in \mathfrak{g}\}$ of $\mathfrak{g} \oplus \mathfrak{g}$) goes over into the adjoint action of G on $\mathfrak{g}$. Theorem II shows that both these actions are variationally complete; these two cases constitute theorems proved in [6], of which our Theorem II is then a generalization.

Chapter III. Applications to Certain Homogeneous Spaces and Loop Spaces.

1. The diagram of K, review of notation. Before stating, in no. 2, our main results, we collect here some facts about Lie groups (cf. [6], [20]).

K is again a compact connected Lie group, with Lie algebra $\mathfrak{k}$; in this chapter, we assume K semi-simple and simply connected. T is a maximal torus in K, with Lie algebra $\mathfrak{t}$; $\dim T = \operatorname{rank} K = l$. On $\mathfrak{k}$ we have the Killing form $(\ ,\ )$, invariant under the adjoint maps $\mathrm{Ad}x$, for all x in K. The orthogonal complement of $\mathfrak{t}$ in $\mathfrak{k}$ is denoted by $\mathfrak{m}$; it splits into m planes of dimension 2, invariant and irreducible under $\mathrm{Ad}T$. If $\mathfrak{e}$ is such a plane with a definite orientation, then there exists a unique linear function $\theta : \mathfrak{t} \to \boldsymbol{R}$, the root belonging to $\mathfrak{e}$, such that $\mathrm{Ad}e^X$, for any $X \in \mathfrak{t}$, operates on $\mathfrak{e}$ as rotation through the angle $2\pi\theta(X)$. It is possible to make a simultaneous choice of orientations for the m planes in such a way that among the corresponding roots θ there are l "fundamental" roots with the property that every θ is a non-negative integral linear combination of the fundamental ones. We assume such a choice made, and call $\mathfrak{R} = \{\theta\}$ the corresponding set of m roots. The dominant root, with all coefficients maximal, we denote by μ. We introduce the set $\mathfrak{P} = \{p\}$ of oriented singular planes in $\mathfrak{t}$; such a plane is by definition a pair (θ, n) of a root θ in $\mathfrak{R}$ and an integer n; for any such pair p, we write p also for the set $\{X \in \mathfrak{t} : \theta(X) = n\}$ and $\bar{p}$ for the image $\exp(p)$ under the exponential map into T or K. Each θ in $\mathfrak{R}$ defines a basic translation τ_θ, the element of $\mathfrak{t}$ that is orthogonal to the plane $(\theta, 0)$ and satisfies $\theta(\tau_\theta) = 2$. We write $\mathfrak{T}$ for the lattice in $\mathfrak{t}$ that the τ_θ generate; $\mathfrak{T}$ is identical with the kernel of the exponential map of $\mathfrak{t}$ into T. For any $p = (\theta, n) \in \mathfrak{P}$, we write $\theta_p = \theta$, $n_p = n$ and $\tau_p = \tau_\theta$. The Cartan integers are defined as the values

$$\theta_p(\tau_q), \text{ for } p, q \in \mathfrak{P}; \tag{1.1}$$

only $0, \pm 1, \pm 2, \pm 3$ occur.

The diagram $D(K)$ is the union of all p in $\mathfrak{P}$; the infinitesimal diagram $D'(K)$ is the union of all $p \in \mathfrak{P}$ with $n_p = 0$. The components of $\mathfrak{t} - D(K)$ are the cells, Δ; the components of $\mathfrak{t} - D'(K)$ are the chambers. We write $\mathfrak{F}$ for the fundamental chamber in which all $\theta \in \mathfrak{R}$ take positive values, and $\Delta_{\mathfrak{F}}$ for the cell in $\mathfrak{F}$ that has the origin 0 in its closure.

Let N_T be the normalizer, in K, of T: The Weyl group $\mathfrak{W}(K)$ or $\mathfrak{W}$ is the (finite) factor group N_T/T. It operates on $\mathfrak{t}$, via the adjoint map, as a group of orthogonal transformations, generated by the reflections across the planes of $D'(K)$; it also operates on T and on K/T (cf. [1]).

2. The main results. The proofs of the results stated here appear in nos. 3-15.

Let s be a line segment in $\mathfrak{t}$, from a point R interior to the fundamental chamber $\mathfrak{F}$ to a point R' interior to the chamber $-\mathfrak{F}$, such that no point of s lies on two or more of the planes of $D'(K)$. Let the roots in $\mathfrak{R}$ be numbered θ_i, $1 \leqq i \leqq m$, in such a way that s meets the planes $(\theta_i, 0)$ in order of increasing index from R to R'. Write τ_i for τ_{θ_i}. Define a graded algebra A_K by

$$A_K = \mathbf{Z}[x_1, \cdots, x_m]/I_m, \tag{2.1}$$

where $\mathbf{Z}[x_1, \cdots, x_m]$ is the polynomial ring over $\mathbf{Z}$ in the variables $x_1, \cdots, x_m$, each x_i of dimension 2, and where I_m is the ideal generated by the elements

$$\rho_k = x_k \cdot (x_k + \sum_1^{k-1} \theta_k(\tau_i) x_i), \qquad 1 \leqq k \leqq m; \tag{2.2}$$

we denote the image of x_i in A_K again by x_i.

Denote by $\mathfrak{d}$ the module of integral forms on $\mathfrak{t}$, i.e. the set of those linear functions on $\mathfrak{t}$ that take integal values at all points of the lattice $\mathfrak{J}$. Finally, let B be the submodule of the linear (two-dimensional) part of A_K formed by the elements of the form $\sum \phi(\tau_i) x_i$ with ϕ ranging over $\mathfrak{d}$.

THEOREM III. *The integral cohomology ring $H^*(K/T)$ of the coset space K/T can be identified with the smallest subring of A_K that* (1) *contains the unit and the module B, and* (2) *is additively a direct summand. In particular, $H^2(K/T)$ is identified with B.*

It is easily seen that B can also be described as follows: Let $\{\zeta_1, \cdots, \zeta_l\}$ be a basis of the lattice $\mathfrak{J}$, and write $\tau_i = \sum a_{ij} \zeta_j$, $1 \leqq i \leqq m$. Then B has as a basis the elements $z_j = \sum a_{ij} x_i$, $1 \leqq j \leqq l$.

We note that this theorem describes the integral cohomology of K/T in terms of infinitesimal invariants of K, namely the Cartan integers and what amounts to the integral relations between the basic translations τ_i (for $\phi \in \mathfrak{D}$, the values $\phi(\tau_i)$ satisfy $\sum a_i\phi(\tau_i) = 0$ whenever $\sum a_i\tau_i = 0$ with real, necessarily rational, a_i).

As an example, we compute G_2/T for the exceptional group G_2. The results III and III′ were announced in [7].

THEOREM III′. *The cohomology ring $H^*(G_2/T)$ contains two elements α, β of dimension 2 such that $H^*(G_2/T)$ has an (additive) basis consisting of* 1, α, β, $\alpha \cdot \beta$, β^2, $\alpha \cdot \beta^2$, $\beta^3/2$, $\alpha \cdot \beta^3/2$, $\beta^4/2$, $\alpha \cdot \beta^4/2$, $\beta^5/2$, $\alpha \cdot \beta^5/2$; *moreover, the relations $\alpha^2 + 3\alpha \cdot \beta + 3\beta^2 = 0$, $\alpha^6 = \beta^6 = 0$ hold.*

Here $\beta^3/2$ means of course an element x such that $2x = \beta^3$.

For any group K, one has the natural action of the Weyl group $\mathfrak{W}$ on K/T and on $H^*(K/T)$. In the description of $H^*(K/T)$, given by Theorem III, this action takes the following form: The operations of $\mathfrak{W}$ on $\mathfrak{t}$ map the lattice $\mathfrak{J}$ into itself. Consequently, there is an induced operation on the module $\mathfrak{D}$ of integral linear forms introduced before Theorem III. Finally, $\mathfrak{W}$ acts on the submodule B of A_K, defined there, since B is naturally isomorphic to $\mathfrak{D}$.

PROPOSITION 2.1. *Under the identification of B and $H^2(K/T)$ of Theorem III, the action of $\mathfrak{W}$ on B becomes identical with the action of $\mathfrak{W}$ on $H^2(K/T)$ derived from the action of $\mathfrak{W}$ on K/T. The action on B extends uniquely to the action on $H^*(K/T)$, the latter considered as a subalgebra of A_K.*

In terms of the bases $\{\zeta_i\}$, $\{z_i\}$ above, we express the image $w \cdot \zeta_i$ of ζ_i under the action of $w \in \mathfrak{W}$ as $\sum b_{ij}\zeta_j$; then the relation $w \cdot z_j = \sum b_{ij}z_i$ defines the operation of w on $H^2(K/T)$.

Let now T' be any non-maximal torus of K, and let $K_{T'}$ (denoted by $C(T')$ in [6]) be the centralizer of T' (a connected group by ([10]). We may assume $T' \subset T$; the latter is then a maximal torus of $K_{T'}$, and the Weyl group $\mathfrak{W}' = \mathfrak{W}(K_{T'})$ is a subgroup of $\mathfrak{W}(K)$.

THEOREM III″. *The cohomology ring $H^*(K/K_{T'})$ is isomorphic to the subalgebra of $H^*(K/T)$, consisting of the invariants of $\mathfrak{W}'$ in $H^*(K/T)$.* (The action of $\mathfrak{W}$, and therefore also of $\mathfrak{W}'$, on $H^*(K/T)$ has been described in Proposition 2.1.).

We note that Theorem III, Proposition 2.1 and Theorem III″ together yield a description of $H^*(K/K_{T'})$ in terms of the Cartan integers, the relations between the basic translations, and the action of the Weyl group of $K_{T'}$ on the basic translations.

The following theorems concern the homotopy groups π_i of Lie groups. It is a classical fact that $\pi_2(K)=0$ for semi-simple K; and it is known [6] that $\pi_3(K)=\mathbf{Z}$ for simple K. We use the standard notation A_n, B_n, C_n, D_n for the classical groups, and G_2, F_4, E_6, E_7, E_8 for the exceptional groups.

THEOREM IV. *Let K be simple and let μ be its dominant root.*

(a) *$\pi_4(K)$ is either 0 or $\mathbf{Z}_2$; it is 0 exactly if the plane $(\mu, 1)$ with equation $\mu(X)=1$ in $\mathfrak{t}$ contains a point of the basic lattice $\mathfrak{I}$.*

(b) *The groups A_1, B_1, and C_n, $n \geqq 1$, have $\pi_4=\mathbf{Z}_2$, all other simple groups have $\pi_4=0$.*

THEOREM V.

(a) $\pi_i(E_6)=0$ for $4 \leqq i \leqq 8$; $\pi_9(E_6)=\mathbf{Z}$;

(b) $\pi_i(E_7)=0$ for $4 \leqq i \leqq 10$; $\pi_{11}(E_7)=\mathbf{Z}$;

(c) $\pi_i(E_8)=0$ for $4 \leqq i \leqq 14$; $\pi_{15}(E_8)=\mathbf{Z}$;

(d) $\pi_{10}(G_2) \otimes \mathbf{Z}_3=0$.

Part (d) is a correction of the value given in Toda's table in [4]; it is in agreement with recent calculations of Toda, and also with recent results of A. Borel-F. Hirzebruch (not yet published).

3. **The groups K_p.** The proofs of the theorems of no. 2 depend on the construction of certain iterated 2-sphere bundles that appear as K-cycles for suitable actions of K.

For each root $\theta \in \mathfrak{R}$, let K_θ be the stabilizer of the singular plane $(\theta, 0)$ of $\mathfrak{t}$, under the adjoint action of K on $\mathfrak{k}$; denote by $\mathcal{K}$ the set of K_θ's. For any oriented singular plane $p \in \mathfrak{P}$, we write K_p for the centralizer of $\bar{p}$ (stabilizer under the action of K on itself by inner automorphisms). It is familiar that for $p=(\theta, n)$, we have $K_p=K_\theta$, independent of n, and that K_p can be described as follows:

Let S_3 denote the special unitary group $SU(2)$ (or equivalently, the group of quaternions of norm 1), topologically a 3-sphere; let S_1 denote the circle group contained in S_3, consisting of the ordinary complex numbers $\cos\phi + i \sin\phi$ in the quaternion form of S_3. For each $p \in \mathfrak{P}$, there exists a monomorphism

$$\beta_p\colon S_3 \rightarrow K_p \tag{3.1}$$

depending only on θ_p and not on n_p, such that T and $\beta_p(S_3)$ generate K_p and such that $\beta_p(S_3) \cap T = \beta_p(S_1)$, cf. [11]. (That β_p is a monomorphism depends on the fact that the element $\frac{1}{2}\cdot\tau_p$ does not belong to the lattice $\mathcal{J}$, and that therefore $\beta_p(-1) \neq e$.) S_3 is a principal bundle for its subgroup S_1, with base space S_2, the 2-sphere (Hopf fibering). Similarly, K_p is a principal T-bundle; β_p is a bundle map, and induces a homeomorphism β_p of the base spaces; we note explicitly that every K_p/T is a 2-sphere.

Let j denote the quaternion unit usually denoted by that letter, and put $j_p = \beta_p(j) \in K_p$. The inner automorphism of K by j_p maps T into itself; its restriction to T is an involution which we denote by R_p. Similarly, $\mathrm{Ad}\,j_p$ maps $\mathfrak{t}$ into itself; its restriction to $\mathfrak{t}$ is also an involution, again denoted by R_p, and given by the formula

$$R_p(X) = X - \theta_p(X)\tau_p, \text{ for } X \in \mathfrak{t} \tag{3.2}$$

(reflection across the plane $(\theta_p, 0)$). The R_p's generate the Weyl group.

Using the standard isomorphism of $\pi_1(T)$ and $H_1(T)$, and the identification of $\pi_1(T)$ with the group $\mathcal{J}$ of covering translations of the universal covering space $\mathfrak{t}$ of T, we associate to each basic translation τ_p or τ_θ a homology class $\boldsymbol{\tau}_p$ or $\boldsymbol{\tau}_\theta$ in $H_1(T)$. For the homology map, induced by R_p, we have then from (3.2),

$$R_{p*}(\boldsymbol{\tau}_q) = \boldsymbol{\tau}_q - \theta_p(\tau_q)\boldsymbol{\tau}_p. \tag{3.3}$$

In particular, on S_1 we have a standard generator $\boldsymbol{\tau}$ of $H_1(S_1)$, such that for the $\beta_p\colon S_1 \to T$, associated with any $p \in P$,

$$\beta_{p*}(\boldsymbol{\tau}) = \boldsymbol{\tau}_p \in H_1(T). \tag{3.4}$$

4. The manifolds Γ_P. Let $P = \{p_1, \cdots, p_r\}$ be an ordered finite sequence of oriented singular planes in $\mathfrak{P}$. Using definition 4.2 of Chapter I, we put

$$\Gamma_P = K_{p_1} \times_T K_{p_2} \times_T \cdots \times_T K_{p_{r-1}} \times_T K_{p_r}/T. \tag{4.1}$$

Our aim is to compute the cohomology of Γ_P. We abbreviate K_{p_i} to K_i, and similarly, θ_{p_i} to θ_i, etc. The polynomial ring $\boldsymbol{Z}[x_1, \cdots, x_r]$ will be considered as a graded ring, the variables having dimension 2.

PROPOSITION 4.2. *The cohomology ring $H^*(\Gamma_p)$ is isomorphic to $\boldsymbol{Z}[x_1, \cdots, x_r]/I_P$, where I_P is the ideal generated by the elements*

$$\rho_k = x_k \cdot \left(x_k + \sum_1^{k-1} \theta_k(\tau_i) x_i\right), \qquad 1 \leqq k \leqq r.$$

In particular, $H^*(\Gamma_P)$ has no torsion and is generated by 2-dimensional elements.

The proof will occupy nos. 4 and 5. The proposition is obvious for $r=1$, since then Γ_P is a 2-sphere (cf. no. 3). We proceed by an inductive construction, and take $r>1$. As in Chapter I, (4.6), we put

$$W_P = K_1 \times \cdots \times K_r. \tag{4.3}$$

The space Γ_P is then also the base space of the principal action of $T^r = T\times\cdots\times T$ (r factors) on W_P, given by

$$(k_1,\cdots,k_r)\cdot(t_1,\cdots,t_r) = (k_1t_1, t_1^{-1}k_2t_2,\cdots,t_{r-1}^{-1}k_rt_r),$$

where $k_i\in K_i$, and $t_i\in T$; let ψ be the projection of W_P onto Γ_P.

Put $P'=\{p_1,\cdots,p_{r-1}\}$, defining $\Gamma_{P'}$, $W_{P'}$ and ψ'. Let $\tilde\phi\colon W_P\to W_{P'}$ be defined by suppressing the last coordinate. This is a bundle map, relative to the homomorphism $\phi\colon T^r\to T^{r-1}$, defined similarly, and induces a map $\bar\phi\colon \Gamma_P\to\Gamma_{P'}$. Writing T^r as $T^{r-1}\times T$, we can factor the projection ψ by first operating on W_P with the factor T, which results in $W_{P'}\times K_r/T$, and then operating with T^{r-1}. One reads off from the basic diagram of Chapter I, (3.1) that Γ_P is the K_r/T-bundle over $\Gamma_{P'}$, associated to the action of T^{r-1} on K/T, given by $(t_1,\cdots,t_{r-1})\cdot k_rT = t_{r-1}k_rT$. Let $\tilde s$ be the natural injection of $W_{P'}$ into $W_P = W_{P'}\times K_r$. One verifies that this is a bundle map, relative to the natural injection of T^{r-1} into $T^r = T^{r-1}\times T$; denote by $\bar s$ the induced map of $\Gamma_{P'}$ into Γ_P. Since $\tilde\phi\circ\tilde s =$ identity, the map $\bar s$ is a cross section of the bundle map $\bar\phi$.

We now set up suitable bases for homology and cohomology. Let $\tilde\chi_i$, for $1\leqq i\leqq r$, denote the map of S_3 into W_P, defined by the β_i (cf. (3.1)) of S_3 into the factor K_i of W_P. This is a bundle map relative to the homomorphism $\chi_i\colon S_1\to T$, given by

$$\chi_i(t) = (e,\cdots,e,\beta_i(t),\cdots,\beta_i(t)),\ \text{with } i-1\ e\text{'s}. \tag{4.4}$$

Let $\bar\chi_i$ be the induced map of S_2 into Γ_P.

We shall apply the transgression map $\partial\colon H_2(\text{base})\to H_1$ (fiber), for the various bundles under consideration; in all cases occurring here, ∂ can be interpreted, via the Hurewicz isomorphism, as the boundary map (dimension 2) of the homotopy sequence of the bundle. We define a generator y of $H_2(S_2)$ by $\partial y=\tau$, where τ is the standard generator of $H_1(T)$ introduced above (cf. (3.4)), and define elements y_i of $H_2(\Gamma_P)$ by

$$y_i = \bar\chi_{i*}(y), \qquad 1\leqq i\leqq r. \tag{4.5}$$

One verifies immediately that the elements y_i, $1 \leqq i \leqq r-1$, map under $\bar{\phi}_*$ into the similarly defined elements y_i', $1 \leqq i \leqq r-1$, of $H_2(\Gamma_{P'})$, that y_r represents a generator of the second homology group of the fiber K_r/T of $\bar{\phi}$, so that $\bar{\phi}_*(y_r)=0$, and that the y_i', $1 \leqq i \leqq r-1$, map into y_i, $1 \leqq i \leqq r-1$, under the cross section $\bar{s}$.

One concludes now inductively by a simple application of the Gysin sequence (for 2-sphere bundles with cross section) (cf. [18]) that the following proposition holds.

PROPOSITION 4.6. *$H^*(\Gamma_P)$ has no torsion (and Γ_P is simply connected). The elements y_i, $1 \leqq i \leqq r$, defined in* (4.5), *form a basis for $H_2(\Gamma_P)$. If ξ is any element of $H^2(\Gamma_P)$ whose restriction to the fiber K_r/T of $\bar{\phi}$ is a generator of $H^2(K_r/T)$, then the map $\bar{\phi}^*$, and the map consisting of $\bar{\phi}^*$ followed by cup-product with ξ are isomorphisms into, and define a direct sum decomposition*

$$H^*(\Gamma_P)=\bar{\phi}^*H^*(\Gamma_{P'}) \oplus \xi \cdot \bar{\phi}^*H^*(\Gamma_{P'}).$$

Specifically, the ring structure of $H^*(\Gamma_P)$ is determined by $H^*(\Gamma_{P'})$ and the expression for ξ^2 in this above decomposition.

Let $\{x_i\}_1{}^r$ be the basis of $H^2(\Gamma_P)$ dual to the basis $\{y_i\}$ of $H_2(\Gamma_P)$ introduced above, so that

$$x_i(y_j)=\delta_{ij}, \qquad 1 \leqq i,j \leqq r. \tag{4.7}$$

The element x_r can then serve as ξ in 4.6. From the properties of the y_i's, it follows at once that the elements x_i, $1 \leqq i \leqq r-1$, are the images under $\bar{\phi}^*$ of the similarly defined elements x_i', $1 \leqq i \leqq r-1$, of $\Gamma_{P'}$, and therefore generate $\bar{\phi}^*H^*(\Gamma_{P'})$, and that

$$\bar{s}^*(x_r)=0. \tag{4.8}$$

5. The involution J.

To find the expression for $x_r{}^2$, we make use of an involution on Γ_P, which reverses the orientation of the fiber. (This method goes back to [12], cf. also [14].) Let $\tilde{J}\colon W_P \to W_P$ be the map sending

$$(k_1,\cdots,k_r) \text{ into } (k_1,\cdots,k_{r-1},k_r\cdot j_r{}^{-1}),$$

where $j_r=\beta_r(j)$ as defined in no. 3. This is a bundle map of the bundle ψ, relative to the map $J\colon T^r \to T^r$, defined by $J(t_1,\cdots,t_r)=(t_1,\cdots,t_{r-1},R_r(t_r))$, with R_r the involution of T determined by conjugation by j_r (cf. no. 3). Let $\bar{J}$ be the induced map of Γ_P into itself. Since $(j_r)^2$ belongs to T, $(\tilde{J})^2$ is a bundle map over the identity and $(\bar{J})^2$ is the identity of Γ_P. Further, since $\tilde{J}$ operates only on the last coordinate of W_P, the map $\bar{J}$ is an involution of the bundle Γ_P over the identity of the base $\Gamma_{P'}$:

$$\bar{\phi} \circ \bar{J} = \bar{\phi}. \tag{5.1}$$

To determine the effect of $\bar{J}$ on $H_2(\Gamma_P)$, we consider, for $1 \leqq i \leqq r$, the map $\bar{\chi}_i \colon S_3 \to W_P$. We write again $T^r = T^{r-1} \times T$; using e_0 as generic symbol for the positive generator of the 0-th homology group (a point with coefficient 1), we have $H_1(T^r) = H_1(T^{r-1}) \otimes e_0 + e_0 \otimes H_1(T)$ [Künneth]. From (4.5), (4.4) and (3.4), we conclude that

$$\partial y_i = \bar{\chi}_{i*}(\boldsymbol{\tau}) = \boldsymbol{\tau}'_i \otimes e_0 + e_0 \otimes \boldsymbol{\tau}_i; \tag{5.2}$$

where the $\boldsymbol{\tau}'_i$ are certain elements of $H_1(T^{r-1})$, with $\boldsymbol{\tau}'_r = 0$. (We have used the fact that the composition of χ_i with the projection of $T^{r-1} \times T$ onto T is just β_i.)

Equivariance with respect to J and $\bar{J}$ shows that

$$\partial \circ \bar{J}_*(y_i) = \boldsymbol{\tau}'_i \otimes e_0 + e_0 \otimes R_{r*}(\boldsymbol{\tau}_i),$$

since J operates only on the last factor of T^r, as R_r. By (3.3), we have

$$\partial(\bar{J}_* y_i) = \boldsymbol{\tau}'_i \otimes e_0 + e_0 \otimes \boldsymbol{\tau}_i - \theta_r(\tau_i) e_0 \otimes \boldsymbol{\tau}_r = \partial(y_i - \theta_r(\tau_i) y_r).$$

The well known fact "$\pi_2(W_P) = 0$" implies that ∂ is an isomorphism into, and we conclude that

$$\bar{J}_*(y_i) = y_i - \theta_r(\tau_i) y_r, \qquad 1 \leqq i \leqq r. \tag{5.3}$$

We note that for $i = r$, this means, because of $\theta_r(\tau_r) = 2$,

$$\bar{J}_*(y_r) = - y_r,$$

so that $\bar{J}$ reverses the orientation of the fiber K_r/T of Γ_P. Going to the dual basis $\{x_i\}$ for $H^2(\Gamma_P)$, we find

$$\bar{J}^*(x_r) = - x_r - \sum_1^{r-1} \theta_r(\tau_i) x_i. \tag{5.4}$$

It follows from the remark at the end of no. 4 that $\bar{J}^*(x_r)$ is congruent to $-x_r \bmod \bar{\phi}^* H^*(\Gamma_{P'})$. Using x_r as the ξ in (4.6), one concludes easily (using also (5.1)) that the elements of $H^*(\Gamma_P)$, invariant under $\bar{J}^*$, are exactly the elements in $\bar{\phi}^* H^*(\Gamma_P)$. We consider now $v = x_r \cdot \bar{J}^*(x_r)$. Since $\bar{J}$ is an involution and $\dim x_r = 2$, we have $\bar{J}^*(v) = v$, and by what was just said, v is of the form $\bar{\phi}^*(u)$. By (4.8), we have $\bar{s}^*(v) = 0$, and therefore $u = \bar{s}^* \circ \bar{\phi}^*(u) = \bar{s}^*(v) = 0$ (since $\bar{\phi} \circ \bar{s} =$ identity), and finally $v = 0$. Writing out $x_r \cdot \bar{J}(x_r)$ from (5.4), we obtain

$$(5.5)\qquad \begin{aligned} &x_r \cdot \Bigl(x_r + \sum_{1}^{r-1} \theta_r(\tau_i)x_i\Bigr) = 0 \quad \text{or} \\ &x_r^2 = -\sum_{1}^{r-1} \theta_r(\tau_i)x_i x_r. \end{aligned}$$

An obvious induction argument, based on (4.6) and the description of $\bar{\phi}^* H^*(\Gamma_P)$, contained in the last sentence of no. 4, completes the proof of (4.2).

6. Description of K/T. We turn to the proof of Theorem III. For this purpose, we consider, as in [6], the adjoint action of K on $\mathfrak{k}$, and apply the considerations of Chapter I. The defect function δ of this action (Chapter I, Definition 7.1)), for points of $\mathfrak{t}$, is determined by the infinitesimal diagram $D'(K)$; namely, $\delta(Q)$ is equal to twice the number of planes in $D'(K)$ that contain Q. This follows readily from the definition of $D'(K)$ and Chapter I, (7.2). In particular, any point of $\mathfrak{t} - D'(K)$ lies on a maximal K-orbit. As the centralizer of such a point is precisely T, its orbit N can be identified with K/T. Let $\alpha\colon K/T \to N$ be such an identification, and consider the space $\Omega_{\mathfrak{k}} = \Omega(\mathfrak{k}; R, N)$, where R is a definite point of $\mathfrak{t} - D'(K)$ not on N. Let $\kappa\colon \Omega_{\mathfrak{k}} \to N$ be the natural projection of paths onto their end points. Because $\mathfrak{k}$ is a Euclidean space, κ induces a homotopy equivalence. Hence $\alpha^{-1} \circ \kappa$ defines a homotopy equivalence: $\Omega_{\mathfrak{k}} \approx K/T$. We will now apply Theorem I to $\Omega_{\mathfrak{k}}$. This is legitimate because of Theorem II.

We recall from [6] that N meets $\mathfrak{t}$ in a finite number of points $Q_1, \cdots, Q_w$ (one in each fundamental chamber). The set $S = S(\mathfrak{k}; R, N)$ consists of the straight line segments s_i from R to the Q_i, and δ_{s_i} is equal to twice the number of planes in $D'(K)$ crossed by s_i. We may assume that the s_i intersect the planes of $D'(K)$ one at a time.

The construction of Chapter I, no. 5, determines K-cycles Γ_i, and maps $f_i\colon \Gamma_i \to \Omega_{\mathfrak{k}}$, for each $s_i \in S$. The stabilizer of a generic point on the plane $(\theta_i, 0)$ is the group $K_{\theta_i} = K_i$ in the system $\mathcal{K}$ defined in no. 3. The Γ_i are therefore of the type considered in no. 4; in particular, each Γ_i is orientable. Hence, by Theorem I, images of the fundamental classes of the Γ_i under $\alpha^{-1} \circ \kappa \circ f_i$ form a basis for the integral homology of K/T.

Since K/T is an orientable manifold it follows that the manifold Γ_{i_0} of highest dimension, $2m$, maps onto K/T with degree ± 1. This K-cycle, to be denoted by Γ_K, is characterized by the fact that R and Q_{i_0} lie in opposite fundamental chambers $\mathcal{F}$ and $-\mathcal{F}$. Adopting the numbering of the roots $\{\theta\}$, described at the beginning of no. 2, with $Q_{i_0} = R'$, we see from Definition 4.1 that

$$\Gamma_K = K_1 \times_T K_2 \times_T \cdots \times_T K_{m-1} \times_T K_m/T, \tag{6.1}$$

The next proposition expresses a general property of maps of degree one; put $f_K = \alpha^{-1} \circ \kappa \circ f_{t_0} \colon \Gamma_K \to K/T$.

PROPOSITION 6.2. *The map* $f_k{}^*$ *maps* $H^*(K/T)$ *isomorphically onto an additively-direct summand of* $H^*(\Gamma_K)$.

Proof. If γ' and γ are suitable fundamental cycles of Γ_K and K/T, we have $f_{K*}(\gamma') = \gamma$, expressing the fact that f_{t_0} is of degree one. We denote by d the Poincaré duality operator, i.e. the cap-product with the fundamental cycle. The permanence relation $f_{K*}(f_K{}^*(a) \cap \gamma') = a \cap f_{K*}(\gamma')$ implies then $f_{K*} \circ d \circ f_K{}^* = d$. Defining $\bar{f} \colon H^*(\Gamma_K) \to H^*(K/T)$ by $\bar{f} = d^{-1} \circ f_{K*} \circ d$, we get $\bar{f} \circ f_K{}^* = d^{-1} \circ d =$ identity, and the proposition follows by standard group theory.

Since $H^*(\Gamma_K)$ has no torsion, Proposition 6.2 gives another proof of the well known fact that K/T has no torsion. [See [6] for references.]

To give the promised description of $H^*(K/T)$, we now make use of an important proposition due to J. Leray and A. Borel [1].

PROPOSITION 6.3. *The cohomology ring* $H^*(K/T; \boldsymbol{Q})$ *over the rationals* $\boldsymbol{Q}$ *is generated by* (*the unit and*) $H^2(K/T; \boldsymbol{Q})$.

The two Propositions 6.2 and 6.3 and the well-known relations between rational and integral cohomology clearly imply the following proposition.

PROPOSITION 6.4. $H^*(K/T)$ *is isomorphic, under* $f_K{}^*$, *to the smallest subalgebra of* $H^*(\Gamma_K)$ *that contains the unit and* $f_K{}^*(H^2(K/T))$ *and is additively a direct summand.*

In Proposition 4.2, we have shown that $H^*(\Gamma_K)$ is the algebra A_K of Theorem III. The theorem will therefore follow from Proposition 6.4, once we have identified the $f_K{}^*$—image of $H^2(K/T)$ in $H^2(\Gamma_K)$. We begin by noting that the transgression ∂ in the bundle $K \to K/T$ maps $H_2(K/T)$ isomorphically onto $H_1(T)$, because of $\pi_1(K) = \pi_2(K) = 0$ (cf. no. 4). Instead of $f_K{}^*$, we consider $\partial \circ f_{K*}$.

PROPOSITION 6.5. *Let* $\{y_i\}_1{}^m$ *be the basis of* $H_2(\Gamma_K)$, *constructed in* 4.5; *the image of* y_i *in* $H_1(T)$ *under* $\partial \circ f_{K*}$ *is* τ_i.

Proof. Let ψ be the bundle projection of the T^m-bundle $W_K = K_1 \times \cdots \times K_n$ onto Γ_K, as in no. 4, and let g be the map of W_K into K, defined by $g(k_1, \cdots, k_m) = k_1 \cdot k_2 \cdot \cdots \cdot k_m$. One verifies that g is a bundle map relative to the projection of T^m onto its last factor T, with K as T-bundle in the usual fashion, and that the induced map of the base spaces is just f_K. For $1 \leqq i \leqq m$, consider the map $\tilde{\chi}_i\colon S_3 \to W_K$. The composition with g is a bundle map, relative to the map $\beta_i\colon S_1 \to T$, over the map $\beta_i\colon S_2 \to K/T$. It follows that

$$\partial \circ f_{K*}(y_i) = \partial \circ f_{K*} \circ \bar{\chi}_i(y) = \partial \circ \bar{\beta}_{i*}(y) = \beta_{i*}(\partial y) = \beta_{i*}(\boldsymbol{\tau}) = \boldsymbol{\tau}_i$$

(by (3.4)).

The map dual to $\partial \circ f_{K*}$ sends the cohomology class $\phi \in H^1(T)$ into the element $\sum \phi(\boldsymbol{\tau}_i) x_i \in H^2(\Gamma_K)$. Each such ϕ can be identified with an integral linear form ϕ on $\mathfrak{t}$ such that $\phi(\boldsymbol{\tau}_i) = \phi(\tau_i)$ (cf. the definition of ϑ before Theorem III and the remark before (3.3)). It is now clear that $f_K{}^* H^2(K/T)$ is the module B of Theorem III.

7. Computation of $H^*(G_2/T)$. As an example, we compute the cohomology of G_2/T, where G_2 is the exceptional group of rank 2. As is customary, we represent the Cartan algebra $\mathfrak{t}$ of G_2 as the plane with equation $t_1 + t_2 + t_3 = 0$ in Euclidean $t_1t_2t_3$-space. The 6-roots θ_i, ordered by the prescription of no. 2 and with a suitable choice of signs, are then given by the expression $t_1 - t_2, t_2, t_2 - t_3, -t_3, t_1 - t_3, t_1$. The corresponding vectors τ_i are given by $(1,-1,0)$, $(-1,2,-1)$, $(0,1,-1)$, $(1,1,-2)$, $(1,0,-1)$, $(2,-1,-1)$. The Cartan integers $\theta_r(\tau_s)$ are given by the matrix

$$\begin{bmatrix} 2 & -3 & -1 & 0 & 1 & 3 \\ -1 & 2 & 1 & 1 & 0 & -1 \\ -1 & 3 & 2 & 3 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 1 & 0 & 1 & 3 & 2 & 3 \\ 1 & -1 & 0 & 1 & 1 & 2 \end{bmatrix}. \tag{7.1}$$

The relations between the variables $x_1, \cdots, x_6$ in the algebra A_{G_2} are then the following:

$$\begin{aligned} x_1{}^2 &= 0 \\ x_2{}^2 &= x_1x_2 \\ x_3{}^2 &= x_1x_3 - 3x_2x_3 \\ x_4{}^2 &= -x_2x_4 - x_3x_4 \\ x_5{}^2 &= -x_1x_5 + x_3x_5 - 3x_4x_5 \\ x_6{}^2 &= -x_1x_6 + x_2x_6 - x_4x_6 - x_5x_6. \end{aligned} \tag{7.2}$$

As basis for the lattice $\mathcal{J}$ spanned by the τ_i, we can take τ_1 and τ_2. The matrix (a_{ij}) is then the matrix of the relations

$$(7.3)\qquad \begin{aligned} \tau_1 &= \tau_1 \\ \tau_2 &= \tau_2 \\ \tau_3 &= \tau_1 + \tau_2 \\ \tau_4 &= 3\tau_1 + 2\tau_2 \\ \tau_5 &= 2\tau_1 + \tau_2 \\ \tau_6 &= 3\tau_1 + \tau_2. \end{aligned}$$

The generators for the image of $H^2(G_2/T)$ in A_{G_2} are therefore

$$\begin{aligned} a &= x_1 + x_3 + 3x_4 + 2x_5 + 3x_6 \\ b &= x_2 + x_3 + 2x_4 + x_5 + x_6. \end{aligned}$$

We change to other generators defined by

$$(7.4)\qquad \begin{aligned} \alpha &= 3b - a = -x_1 + 3x_2 + 2x_3 + 3x_4 + x_5 \\ \beta &= a - 2b = x_1 - 2x_2 - x_3 - x_4 + x_6. \end{aligned}$$

One verifies the relations

$$(7, 5)\qquad \begin{aligned} &\text{a)} \quad \alpha^2 + 3\alpha\beta + 3\beta^2 = 0, \\ &\text{b)} \quad \beta^3 \text{ divisible by } 2, \\ &\text{c)} \quad \alpha \cdot \beta^5 = 2x_1 \cdot x_2 \cdot \cdots \cdot x_6, \\ &\text{d)} \quad \alpha^6 = \beta^6 = 0. \end{aligned}$$

Relation (7.5a)) shows that the products of the form β^t, $\alpha \cdot \beta^t$, $0 \leqq t \leqq 5$, span $f^*(H^*(G_2/T))$ rationally, i. e. up to division by integers. The product $x_1 \cdot \cdots \cdot x_6$ represents the fundamental cocycle of Γ_{G_2}. It follows from (7.5c)) that all divisibility relations in $H^*(G_2/T)$ are consequences of (7.5b)), and that a basis for $H^*(G_2/T)$ is given by

$$\{1, \alpha, \beta, \alpha \cdot \beta, \beta^2, \alpha \cdot \beta^2, \beta^3/2, \alpha \cdot \beta^3/2, \beta^4/2, \alpha \cdot \beta^4/2, \beta^5/2, \alpha \cdot \beta^5/2\}.$$

This completely determines the cohomology ring $H^*(G_2/T)$, and proves Theorem III′. The computations are facilitated by making the change of variables:

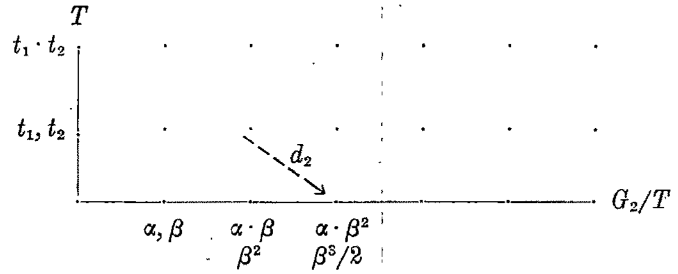
$$(7.6)\qquad \begin{aligned} y_1 &= x_1 \\ y_2 &= x_2 \\ y_3 &= -2x_1 + 3x_2 + x_3 \\ y_4 &= -x_1 + 2x_2 + x_3 + x_4 \\ \alpha &= -x_1 + 3x_2 + 2x_3 + 3x_4 + x_5 \\ \beta &= x_1 - 2x_2 - x_3 - x_4 + x_6. \end{aligned}$$

The relations (7.2) go over into

$$\begin{aligned} y_1{}^2 &= 0 \\ y_2{}^2 &= y_1y_2 \\ y_3{}^2 &= 3y_1y_2 - 3y_1y_3 + 3y_2y_3 \\ y_4{}^2 &= -\tfrac{1}{3}y_3{}^2 + y_3y_4 \\ \alpha^2 &= -3y_4{}^2 + 3y_4\cdot\alpha \\ \beta^2 &= \tfrac{1}{3}\alpha^2 + \alpha\beta. \end{aligned} \tag{7.7}$$

It is clear that $x_1 \cdot \cdots \cdot x_6 = y_1y_2y_3y_4\alpha\beta$.

As an application, one verifies, by a standard computation with the spectral sequence of $G_2 \rightarrow G_2/T$, that $H^*(G_2)$ has $\mathbf{Z}_2$ as torsion group in dimensions 6 and 9, as found by Borel in [3].



Note that the differential indicated above has $\mathbf{Z}_2$ as cokernel: $\beta^3/2$ is not in the image, although, with $d_2t_1 = \alpha$, $d_2t_2 = \beta$, one has $d_2(\beta^2 \cdot t_2) = 2 \cdot \beta^3/2$.

8. Cohomology of $K/K_{T'}$. We continue to use the notation introduced in no. 6. The proof of Proposition 2.1, to which we turn now, depends on the fact that the transgression $\partial \colon H_2(K/T) \rightarrow H_1(T)$, is equivariant with respect to the operation of the Weyl group, and that the same holds for the dual map ∂^* of the cohomology groups. This proves the statement about the action of $\mathfrak{W}$ on B, as a consequence of the remarks at the end of no. 6. The uniqueness of the extension to all of $H^*(K/T)$ follows from Theorem III. Note that $\mathfrak{W}$ does not act as a group of automorphisms on A_K.

The proof of Theorem III″ goes along quite different lines. We consider the spectral sequence of the fiber map $K/T \rightarrow K/K_{T'}$, with fiber $K_{T'}/T$, induced by the inclusions $K \supset K_{T'} \supset T$. All dimensions in $H^*(K/K_{T'})$ and in $H^*(K_{T'}/T)$ are even, and the spectral sequence is trivial (all differentials vanish). The Weyl group $\mathfrak{W}'$ of $K_{T'}$ operates on the spectral sequence. The operation is trivial on the base space $K/K_{T'}$, since $K_{T'}$ is connected. The operation on $H^*(K_{T'}/T)$ is known to be equivalent to the regular representation of $\mathfrak{W}'$ (cf. [1]); the elements left fixed by all $w \in \mathfrak{W}'$ are exactly the elements of $H^0(K_{T'}/T)$. It follows now by comparing the E_2-term $H^*(K/K_{T'}) \otimes H^*(K_{T'}/T)$ with $H^*(K/T)$, that $H^*(K/K_{T'})$ [considered as a subalgebra of $H^*(K/T)$] consists exactly of the elements of $H^*(K/T)$ left fixed by all $w \in \mathfrak{W}'$, and Theorem III″ is proved.

9. The holomogy of $\boldsymbol{\Omega}(K)$; applications to homotopy. Let K operate on itself by inner automorphisms. Let R be a point of K, and let $\Omega_R = \Omega(K; R, e)$ be the space of paths, as in Chapter I, no. 2, from R to the orbit of e, i. e. to e. Ω_R can be identified, in standard fashion, with the space $\Omega(K) = \Omega(K; e, e)$ of loops in K at e; since K is simply connected, this identification is unique up to homotopy.

Suppose now that R is a regular point of T, i. e. supposes $R \notin \bar{p}$ for any $p \in \mathfrak{P}$; the orbit of R is then of maximal dimension, and because of Theorem II, we can apply Theorem I to Ω_R. As shown in [6], the set $S = S(K; R, e)$ of Chapter I, no. 2, can be identified with the set S' of line segments in $\mathfrak{t}$, obtained by choosing in each cell Δ of the fundamental chamber $\mathfrak{F}$ a suitable point, and connecting it to the origin 0 by a straight segment s. To Δ or to s, we associate the K-cycle of the geodesic segment $\exp \circ s$ (in the sense of Chapter I, no. 4), denoted by Γ_Δ, and the map of Γ_Δ into $\Omega(K)$ (using the identification of the various Ω_R above), denoted by f_Δ. The exceptional points of $\exp \circ s$ correspond to the points where s crosses singular planes in $\mathfrak{t}$ (we assume that s has no point of higher singularity). The exceptional stabilizers are then groups of the set $\mathcal{K}$ of no. 3; the stabilizer of $\exp \circ s$ is T itself. It follows that all K-cycles are of the type discussed in no. 4. In more detail, we get from Theorem I the following proposition, describing the homology of $\Omega(K)$.

PROPOSITION 9.1. *For each cell Δ in $\mathfrak{F}$, let $P = \{p_1, \cdots, p_r\}$ be the ordered set of oriented planes in $\mathfrak{P}$ that the segment s from Δ to 0 crosses (in that order). The K-cycle Γ_Δ is then Γ_P, in the sense of* 4.1, *so that in particular* $\dim \Gamma_\Delta = 2r$. *The f_Δ-images of fundamental cycles γ_Δ of the Γ_Δ, with Δ ranging over the cells of $\mathfrak{F}$, form a basis for the (free) group* $H_*(\Omega(K))$.

It should be noted that strictly speaking the geodesic segment $\exp \circ s$ is not in the set S, but that a suitable inner automorphism of K will bring it into S. The abstract K-cycle will not change under this operation; and, K being connected, the image homology class in the loop space will also be the same (using again the identification of all the Ω_R).

For our application to homotopy, we need a partial determination of the cohomology ring of $\Omega(K)$. We quote some well known facts. Assume from now on K to be simple. The cohomology $H^*(K;\boldsymbol{Q})$ over the rationals $\boldsymbol{Q}$ is an exterior algebra with l generators of dimensions $2m_i-1$, with $2=m_1<m_2\leqq\cdots\leqq m_l$ (actually $m_2=m_3$ only for the type D_4). The cohomology $H^*(\Omega(K);\boldsymbol{Q})$ is a polynomial ring with l generators of dimensions $2m_i-2$. Since $H^*(\Omega(K))$ has no torsion, this implies that all $H^{2i+1}(\Omega(K))$ vanish, that $H^{2i}(\Omega(K))$ is infinite cyclic for $0\leqq i\leqq m_2-2$, and that $H^{2m_2-2}(\Omega(K))$ is free abelian of rank 2 or 3. Let η denote a generator of $H^2(\Omega(K))$; no power η^i vanishes. The second non-vanishing homotopy group of K (or $\Omega(K)$) depends on the divisibility properties (by integers) of the powers η^i, $2\leqq i\leqq m_2-1$, as described in the next proposition.

PROPOSITION 9.2. (A) *Suppose no power* η^i, *for* $1\leqq i\leqq m_2-1$, *is divisible by an integer* >1; *then* $\pi_r(K)=0$ *for* $3<r<2m_2-1$, *and* $\pi_{2m_2-1}(K)$ *is free abelian of rank one less than the number of* m_i*'s equal to* m_2;

(B) *In the remaining case, let* i_0 *be the smallest exponent* $i\leqq m_2-1$ *for which* η^i *is divisible, and let* η^{i_0} *be divisible exactly by the positive integer* q (>1); *then* $\pi_r(K)=0$ *for* $3<r<2i_0$, *and* $\pi_{2i_0}(K)=\boldsymbol{Z}_q$.

Proof. The integral cohomology ring of the Eilenberg-MacLane space $K(\boldsymbol{Z},2)$, the infinite complex projective space, is a polynomial ring $\boldsymbol{Z}[x]$ with $\dim x=2$. By standard principles, there exists a map $\phi_\eta\colon\Omega(K)\to(\boldsymbol{Z},2)$ such that $\phi_\eta{}^*(x)=\eta$, and consequently $\phi_\eta{}^*(x^i)=\eta^i$. One can now easily determine the nature of the first non-vanishing relative homology group of ϕ_η (i.e. of the mapping cylinder of ϕ_η, with $\Omega(K)$ as the subset) in terms of the assumptions in (9.2); the Hurewicz isomorphism theorem and the known nature of the $\pi_r(K(\boldsymbol{Z},2))$ yield then (9.2). We see from (9.1) that η^i is divisible by q exactly if for every Δ with $\dim\Gamma_\Delta=2i$, the cocycle $f_\Delta{}^*(\eta^i)$ (a multiple of the fundamental cocycle of Γ_Δ) is divisible by q. We shall study this question using the description of Γ_Δ in (4.2), and begin by finding the expression for $f_\Delta{}^*(\eta)$.

10. The 3-spheres in *K*.

We identify the Lie algebra of the subgroup S_1 of the group S_3 (cf. no. 3) with the real numbers $\boldsymbol{R}$ such that the exponential map is given by $\phi\to e^{i\phi}$, for $\phi\in\boldsymbol{R}$. There is then one root θ with $\theta(\phi)=\frac{1}{\pi}\phi$; the basic translation τ_θ is the number 2π; the system $\mathfrak{P}$ of oriented singular planes can be identified with the integral multiples of π; the fundamental chamber is given by $\phi > 0$. Let n be any integer; let $s\colon [0,1] \to \mathbf{R}$ be a non-degenerate, linear map with $s(1) = 0$ such that for some $\bar{t} \in [0,1)$, we have $s(\bar{t}) = n \cdot \pi$, so that $\bar{t}$ is an exceptional value of the geodesic segment $\exp \circ s$ in S_3, according to Chapter I, no. 4. Put $R = \exp \circ s(0)$. We write $s = s' + s''$ with $s' = [0, \bar{t}]$ (possibly degenerate) and $s'' = [\bar{t}, 1]$. Generalizing slightly the construction of Chapter I, no. 5, we define a map $\bar{f}_n\colon S_3 \to \Omega(S_3; R, 1)$ by $\bar{f}_n(x) = \exp \circ s' + x \cdot \exp \circ s'' \cdot x^{-1}$. This is well defined at the junction point since the centralizer of $\exp \circ s(\bar{t})$ is S_3. As in Chapter I, no. 5, the map $\bar{f}_n$ is constant along the cosets of S_1, and induces a map $f_n\colon S_2 = S_3/S_1 \to \Omega(S_3; R, 1)$.

PROPOSITION 10.1. *Let y be the generator of $H_2(S_2)$ defined in* 3.3. *Then $\bar{y} = f_{1*}(y)$ is a generator of the infinite cyclic group $H_2(\Omega(S_3))$; and $f_{n*}(y) = n \cdot \bar{y}$.*

We identify here $\Omega(S_3; R, 1)$ with $\Omega(S_3) = \Omega(S_3; 1, 1)$; that $\bar{y}$ is a generator of $H_2(\Omega(S_3))$ is a special case of Proposition 9.1 for $K = S_3$, since the interval $(\pi, 2\pi)$ is the only cell Δ whose Γ_Δ has dimension 2, and since S_2 and f_1 are just the associated Γ_Δ and f_Δ.

To treat the factor n, we note first that we may choose s in such a way that $s(0) = 2n\pi$. Let ρ be the natural homomorphism of S_3 onto $S_3/\{1, -1\} = P_3$ (projective 3-space $= SO(3)$). Each $\rho \circ f_n(x)$, for $x \in S_2$, is then a loop in P_3 that goes through e at the parameter values $i/2n$, $0 \leqq i \leqq 2n$; in other words, it is a $2n$-fold Pontryagin product in $\Omega(P_3)$. Using the fact that the Pontryagin product in the loop space of a group is homotopy-commutative one verifies that $\rho \circ f_n$ is homotopic to the n-th Pontryagin power of $\rho \circ f_1$ (for $n \geqq 0$), and to the inverse of $\rho \circ f_1$ for $n = -1$. Since ρ induces a homeomorphism of $\Omega(S_3)$ with the e-component of $\Omega(P_3)$, and since y, being spherical, is primitive, one concludes now easily that $f_{n*}(y) = n \cdot \bar{y}$.

For any root $\theta \in \mathfrak{R}$, let $g_\theta\colon S_3 \to K$ be the composition of the map β_θ of no. 3 with the inclusion of K_θ in K, and let $\bar{g}_\theta$ be the induced map of the loop spaces.

PROPOSITION 10.2. (A) *The element $\bar{g}_{\mu*}(\bar{y}) = y_K$ (where μ is the dominant root and $\bar{y}$ is defined in* 10.1) *is a generator of $H_2(\Omega(K))$.*

(B) *For any root $\theta \in \mathfrak{R}$, the following relation holds:*

$$\bar{g}_{\theta*}(\bar{y}) = ((\tau_\theta, \tau_\theta)/(\tau_\mu \cdot \tau_\mu)) \cdot y_K.$$

(Note that the factor of y_K is always an integer.)

For part (A), we use (9.1). There is exactly one cell Δ in $\mathfrak{S}$ with

$\dim \Gamma_\Delta = 2$, namely the cell obtained by reflecting the fundamental cell $\Delta_{\mathfrak{F}}$ across the plane $(\mu, 1)$; we have $\Gamma_\Delta = K_\mu/T$. One verifies, by considering the definition of f_Δ, Chapter I, no. 5, the relation

$$f_\Delta \circ \bar{\chi}_1 = \bar{g}_\mu \circ f_1, \tag{10.3}$$

with f_1 as defined above, and $\bar{\chi}_1 : S_2 \rightarrow \Gamma_\Delta$ defined in no. 4. [Actually, this equation has to be understood as a homotopy. The map f_Δ is defined by a certain segment s in $\mathfrak{t}$. As far as $f_\Delta \circ \bar{\chi}_1$ goes, one can replace s by any segment in $\mathfrak{t}$ that has 0 as end point and for whose initial point the inequality $\mu(s(0)) \geqq 1$ holds, provided that one disregards all exceptional points of s except the one where s meets the plane $(\mu, 1)$. In terms of Chapter I, no. 5, this means that instead of W_n we act on s only with $T \times \cdots \times T \times K_n$. It is now possible to take for s the image, under the differential $\dot{g}_\mu$ of g_μ, of the segment used for the construction of f_1 in the Lie algebra $\boldsymbol{R}$ of S_1; this produces actual equality in the above relation.] It follows that $f_{\Delta *}(y_1) = \bar{g}_{\mu *}(\bar{y})$; since y_1 is the fundamental cycle of K_μ/T, part (A) follows.

The standard transgression argument shows that, with z denoting a generator of $H_3(S_3)$, the element $g_{\mu *}(z)$ is a generator of $H_3(K)$. We shall prove (10.2 (B)) by showing that $g_{\theta *}(z) = ((\tau_\theta, \tau_\theta)/(\tau_\mu, \tau_\mu)) \cdot g_{\mu *}(z)$.

Let ψ_K be the Cartan-form of K, i.e. the closed invariant differential 3-form defined, at e, by $\psi_K(X, Y, Z) = (X, [Y, Z])$. Let τ, τ', τ'' be a basis for the Lie algebra of S_3, with τ the basic translation in the Lie algebra of S_1, and $[\tau', \tau''] = \tau$. By (3.4), we have $\beta_\theta(\tau) = \tau_\theta$, and therefore $g_\theta{}^* \psi_K(\tau, \tau', \tau'') = (\tau_\theta, \tau_\theta)$. This implies $g_\theta{}^* \psi_K = ((\tau_\theta, \tau_\theta)/(\tau_\mu, \tau_\mu)) \cdot g_\mu{}^* \psi_K$, and (10.2 (B)) follows.

11. Computation of $f_\Delta{}^*(\eta)$.

Let the generator η of $H^2(\Omega(K))$ be so chosen that $\eta(y_K) = 1$, with y_K as in (10.2(A)). Let Δ be any cell in $\mathfrak{F}$, and let $P = \{p_1, \cdots, p_r\}$, Γ_Δ and f_Δ be as in (9.1). By no. 4, to each $p_i \in P$, there corresponds a basis element y_i of $H_2(\Gamma_\Delta)$; the determination of $f_\Delta{}^*(\eta) \in H^2(\Gamma_\Delta)$ is equivalent to that of $f_{\Delta *}(y_i)$, $1 \leqq i \leqq r$.

PROPOSITION 11.1.

$$f_{\Delta *}(y_i) = n_i((\tau_i, \tau_i)/(\tau_\mu, \tau_\mu)) \cdot y_K,$$

with $\tau_i = \tau_{p_i}$ *and* $n_i = n_{p_i}$, *the translation and the multiplicity associated with the singular plane* p_i.

For the proof, one verifies, as in the proof of (10.2), that the commutativity relation $f_\Delta \circ \bar{\chi}_i = \bar{g}_i \circ f_{n_i}$ holds, where f_{n_i} is as in (10.1), and where $\bar{g}_i$

is the map of the loop spaces induced by the map $g_i\colon S_3 \to K_i \subset K$. (11.1) follows then from (10.1) and (10.2 (B)). By simple duality, we have

PROPOSITION 11.2.

$$f_\Delta^*(\eta) = (\tau_\mu, \tau_\mu)^{-1} \sum_1^r n_i (\tau_i, \tau_i) x_i;$$

here τ_i, n_i *are the basic translation and the multiplicity associated with the i-th singular plane* p_i *along the segment* s *from* Δ *to* 0.

12. Computation of $\pi_4(K)$. To determine $\pi_4(K)$, we have to consider the element η^2, according to (9.2); according to (9.1), this amounts to considering all cells Δ with $\dim \Gamma_\Delta = 4$. Assume that the rank l of K is > 1. Let Δ_1 be the cell obtained from the fundamental cell $\Delta_{\mathfrak{F}}$ by reflection across the plane $(\mu, 1)$. It is clear that the cells that correspond to dimension 4 are the cells in $\mathfrak{F}$ adjoining to Δ_1 (different from $\Delta_{\mathfrak{F}}$). Let Δ be such a cell (actually there are one or two such, with two occurring for the type A_n, $n \geqq 2$, only). The segments from Δ to 0 has 2 exceptional points; the first belongs to a certain root, say θ; the second belongs to the dominant root. By (4.2), the ring $H^*(\Gamma_\Delta)$ is then generated by two variables x_1, x_2 subject to $x_1^2 = 0$ and $x_2^2 = -a x_1 x_2$, where $a = \mu(\tau_\theta)$. The multiplicities n_1, n_2 of (11.2) are both 1, and we have $f_\Delta^*(\eta) = ((\tau_\theta, \tau_\theta)/(\tau_\mu, \tau_\mu)) \cdot x_1 + x_2$. Squaring, we obtain

$$f_\Delta^*(\eta^2) = (2(\tau_\theta, \tau_\theta)/(\tau_\mu, \tau_\mu) - a) x_1 x_2.$$

Since τ_μ belongs to the closure of $\mathfrak{F}$, we have $\theta(\tau_\mu) > 0$ ($\neq 0$, since τ_μ and τ_θ are clearly not orthogonal). Moreover, since $(\tau_\mu, \tau_\mu) \leqq (\tau_\theta, \tau_\theta)$ (τ_μ is a "shortest" translation), we have $\theta(\tau_\mu) < \theta(\tau_\theta) = 2$, and so $\theta(\tau_\mu) = 1$. It follows that $(\tau_\theta, \tau_\theta)/(\tau_\mu, \tau_\mu) = \mu(\tau_\theta)/\theta(\tau_\mu) = \mu(\tau_\theta)$, and so

$$f_\Delta^*(\eta^2) = \mu(\tau_\theta) x_1 x_2 \tag{12.1}$$

It follows from (12.1) that η^2 is divisible by the integer $q \geqq 1$ if and only if the Cartan integers $\mu(\tau_\theta)$, for the θ's involved, are so divisible. Recalling that these roots θ are obtained by reflecting across the plane $(\mu, 1)$ those fundamental roots that are not orthogonal to μ, and recalling that the translations belonging to the fundamental roots generate the lattice $\mathfrak{T}$, one sees easily that η^2 is divisible by q exactly if all values $\mu(X)$, for $X \in \mathfrak{T}$, are so divisible. Since $\mu(\tau_\mu) = 2$, this means $q = 1$ or 2. Moreover, q will be 1 exactly if there exists an $X \in \mathfrak{T}$ with $\mu(X) = 1$. This proves Theorem IV(a). The statements of IV(b) are obtained by a simple inspection of the diagrams of the simple groups. The case $l = 1$, i. e. the group S_3 itself, can be treated with the same method; there is only one root, the multiplicity n_1 is 2, as is the Cartan integer x; n_2 is 1; $f_\Delta{}^*(\eta) = 2x_1 + x_2$; $f_\Delta{}^*(\eta^2) = 2x_1x_2$. The result $\pi_4(S_3) = \boldsymbol{Z}_2$ is of course well known

13. Homotopy groups of E_6, E_7, E_8. To have a way of picturing the arrangement of the cells in the fundamental chamber, we associate to the Lie group K a graph $\Phi = \Phi(K)$, the 1-skeleton of the dual of the triangulation of $\mathfrak{F}$ by the cells, with labelled edges. To each cell Δ in $\mathfrak{F}$, there is associated a vertex v_Δ, and to any $(l-1)$-face between two cells is associated an edge connecting the two vertices; the edge is labelled with the plane $p \in \mathfrak{P}$ in which the $(l-1)$-face lies. There is a distinguished vertex $v_{\mathfrak{F}}$, corresponding to the lowest cell $\Delta_{\mathfrak{F}}$. We define a function d of the vertices by setting $d(v) =$ smallest number of edges in a path from v to $v_{\mathfrak{F}}$. One verifies that for any cell Δ with segment s from Δ to 0 and K-cycle Γ_Δ, as in (9.1), one has $\dim \Gamma_\Delta = 2d(v_\Delta)$, and that the singular planes occur along s in the same order as along a *suitable* minimal path from v_Δ to $v_{\mathfrak{F}}$ in Φ. We write Φ_i for the subgraph of Φ containing all vertices with d-values $\leqq i$.

Then, for any K $(\neq D_4)$, the graph Φ_{m_2-1} (here m_2 is the second primitive exponent of K, cf. no. 9) has the form

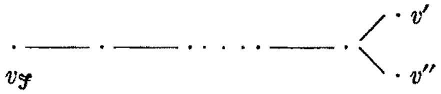


Figure 2.

as follows at once from the behavior of the Betti numbers. Since for all the vertices shown, the minimal path to $v_{\mathfrak{F}}$ is unique, one can read off the nature of the K-cycles Γ_Δ, provided one knows which planes of $\mathfrak{P}$ are attached to the various edges. The first edge (i. e., the edge at $v_{\mathfrak{F}}$) is of course labelled with the dominant root μ, or better, with the plane $(\mu, 1)$. We now describe the labelling of Φ_{m_2-1} for the exceptional groups E_6, E_7, E_8, in terms of the usual fundamental roots $\{\phi_i\}_1{}^l$ (cf. the Coxeter (Schläfli) diagrams below). To have a short description, we state first that all the planes p occurring are of the form $(\theta, 1)$, i. e. they have $n_p = 1$. Further, it turns out that for each edge after the first one, the root attached is obtained by subtracting a suitable fundamental root from the root attached to the edge immediately preceding in Φ. We give below the system consisting of the dominant root and the fundamental roots to be subtracted successively; the last two entries correspond to the two edges leading to v' and v''.

$$\begin{array}{l} E_6:\ \{\mu, \phi_6, \phi_3 ; \phi_2, \phi_4\} \\ E_7:\ \{\mu, \phi_6, \phi_5, \phi_4 ; \phi_3, \phi_7\} \\ E_8:\ \{\mu, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5 ; \phi_6, \phi_8\}. \end{array} \tag{13.1}$$

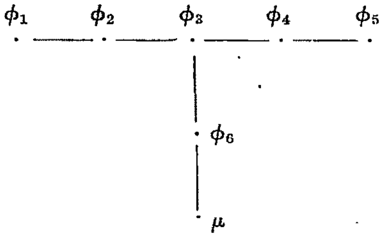
The singular plane attached to the 3rd edge of $\Phi_4(E_6)$, e.g., is then $(\mu - \phi_6 - \phi_3, 1)$; the plane attached to the edge leading to v' is $(\mu - \phi_6 - \phi_3 - \phi_2, 1)$. To prove that these are the correct values, we proceed as follows:

(A) The fundamental roots indicated in (13.1), are the only ones at each stage in the processe that can be subtracted from the root obtained up to the point in question and yield again a root as difference. To verify this we start from the remark that for any two roots θ, θ' of a group K, the difference $\theta - \theta'$ is again a root if $\theta'(\tau_\theta)$ is positive (cf. [5]); moreover, for E_6, E_7, E_8 the reverse implication is also true, since all basic translations are of the same length, say 1. Further, we have for the fundamental roots ϕ_i and the corresponding basic translations λ_i the usual relations

$$\begin{array}{l} \phi_i(\lambda_i) = 2, \\ \phi_i(\lambda_j) = 2(\lambda_i, \lambda_j) = -1, \text{ if } \phi_i \text{ and } \phi_j \text{ are adjacent in the Coxeter diagram,} \\ \phi_i(\lambda_j) = 0 \text{ otherwise.} \end{array} \tag{13.2}$$

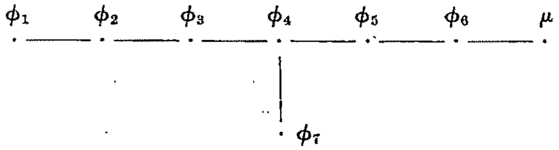
One verifies that in our three cases the dominant root μ has $\mu(\lambda_i)$ positive for exactly one of the λ_i, and 0 for all others, so that exactly one $\mu - \phi_i$ is a root (cf. also [5]). We reproduce the three Coxeter diagrams, with in each case a new vertex, corresponding to the dominant root, joined by an edge to the unique vertex whose corresponding λ_i is not orthogonal to τ_μ.

E_6:



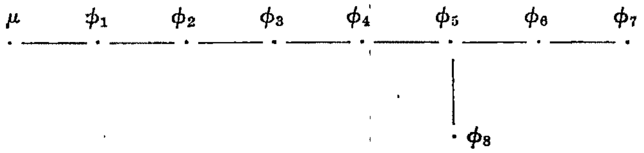
$$\mu = \phi_1 + 2\phi_2 + 3\phi_3 + 2\phi_4 + \phi_5 + 2\phi_6,$$

E_7:



$$\mu = \phi_1 + 2\phi_2 + 3\phi_3 + 4\phi_4 + 3\phi_5 + 2\phi_6 + 2\phi_7,$$

E_8:



$$\mu = 2\phi_1 + 3\phi_2 + 4\phi_3 + 5\phi_4 + 6\phi_5 + 4\phi_6 + 2\phi_7 + 3\phi_8.$$

As an example, we compute, for E_6, $\mu(\lambda_1) = \phi_1(\lambda_1) + 2\phi_2(\lambda_1) = 2 - (2 \cdot -1) = 0$ and $\mu(\lambda_6) = 3\phi_3(\lambda_6) + 2\phi_6(\lambda_6) = 3 \cdot -1 + 2.2 = 1$. One verifies the statement made in (A) about the roots in 13.1 directly from the diagrams. As an example, for E_6, to find a ϕ_i for which $\mu - \phi_6 - \phi_i$ is a root, we have to find a ϕ_i for which $\phi_i(\tau_\mu - \lambda_6) = \phi_i(\tau_\mu) - \phi_i(\lambda_6) > 0$. Clearly i must be different from 6; but then $\phi_i(\tau_\mu) = 0$, and the only root with $\phi_i(\lambda_6) \neq 0$ (and actually $= -1$ by (13.2)) is the root ϕ_3, adjacent to ϕ_6.

(B) If for two planes $p = (\theta, n)$, $p' = (\theta', n')$ of $\mathfrak{P}$, the linear function $\theta/n - \theta'/n'$ is positive on $\mathcal{F}$, then clearly the first (i.e. nearest to $v_{\mathcal{F}}$) occurrence of p at an edge of Φ comes before any occurrence of p'. One verifies now that the roots θ constructed by the prescription in (13.1), are successively smaller in this sense, since each time a fundamental root is subtracted (except that the last two roots are not comparable in this ordering), and that they are all greater than $\frac{1}{2}\cdot\mu$ (by explicit computation; e.g., for E_6, $\mu - \phi_6 - \phi_3 - \phi_2 = \phi_1 + \phi_2 + \phi_3 + 2\phi_4 + \phi_5 + \phi_6 > \frac{1}{2}\cdot\mu$ on $\mathcal{F}$).

It is clear from (A) and (B) that the labelling of Φ_{m_2-1}, described by (13.1), is the correct one.

For each of E_6, E_7, E_8, we shall now compute the cohomology ring of the manifold Γ', attached by (9.1) to the vertex v' of the graph Φ_{m_2-1}, and also the image, under the associated map f', of η (by (11.2)) and of the relevant power of η; using (9.2), this will yield Theorem V(a), (b), (c). If s is a segment from the cell Δ', corresponding to v' in figure 2, to 0, then the singular planes crossed by s are identical with the singular planes attached to the edges of Φ_{π_2-1}, moving from v' to $v_{\mathcal{F}}$. All the multiplicities are 1, as noted before; all the "weights" $(\tau_i, \tau_i)/(\tau_\mu, \tau_\mu)$ occurring in (11.2) are also 1. The roots along s are given by the description in (13.1) (but in reverse order!). For E_6, for instance, the singular planes p_1, p_2, p_3, p_4 are given by $(\mu - \phi_6 - \phi_3 - \phi_2, 1)$, $(\mu - \phi_6 - \phi_3, 1)$ $(\mu - \phi_6, 1)$ $(\mu, 1)$.

It turns out that all the Cartan integers, appearing in the description (4.2) of the cohomology of our Γ's are 1. As an example, for E_6, the integer $\mu(\tau_\mu - \lambda_6) = \mu(\tau_\mu) - \mu(\lambda_6) = 2 - 1 = 1$. We omit the details.

For the Γ' of E_6, the cohomology is then generated by variables x_1, x_2, x_3, x_4, with the relations

$$\begin{aligned} &x_1^2 = 0, \\ &x_2(x_1 + x_2) = 0, \\ &x_3(x_1 + x_2 + x_3) = 0, \\ &x_4(x_1 + x_2 + x_3 + x_4) = 0, \end{aligned} \tag{13.1}$$

and $f'^*(\eta)$ is given by $x_1 + x_2 + x_3 + x_4$. The fundamental cocycle of Γ' is given by $x_1x_2x_3x_4$; we claim

$$f'^*(\eta^4) = x_1x_2x_3x_4. \tag{13.4}$$

For the (elementary) computation, we introduce a new basis by setting $z_1 = x_1$, $z_1 = x_1 + x_2$, $z_3 = x_1 + x_2 + x_3$, $z_4 = x_1 + x_2 + x_3 + x_4$. The relations turn into

$$\begin{aligned} &z_1^2 = 0,\ z_2^2 = z_1z_2,\ z_3^2 = z_2z_3,\ z_4^2 = z_3z_4, \\ &\text{and } f'^*(\eta) \text{ is given by } z_4. \end{aligned} \tag{13.5}$$

Now $(z_4)^4 = (z_3z_4)^2 = z_2z_3^2 \cdot z_4 = z_2^2 \cdot z_3z_4 = z_1z_2z_3z_4 = x_1x_2x_3x_4$, q. e. d.

It follows that the powers η^i, $1 \leqq i \leqq 4$, are not divisible by any integers $q > 1$, and Theorem V(a) follows from (9.2).

The computations for E_7 and E_8, with 5, resp. 7 variables x_i are entirely analogous.

14. $\pi_{10}(G_2) \otimes \boldsymbol{Z}_3$, preparation.

Following a suggestion of J. C. Moore and A. S. Shapiro, we shall compute $\pi_{10}(G_2) \otimes \boldsymbol{Z}_3$ by considering, in addition to the ring structure of $H^*(\Omega(G_2); \boldsymbol{Z}_3)$ up to dimension 10, a certain Steenrod power (cf. [19] for this concept).

We begin by listing the necessary facts about G_2 (in a notation somewhat different from no. 7).

(1) Fundamental roots ϕ_1, ϕ_2; corresponding translations λ_1, λ_2;

(2) Coxeter diagram $\overset{\phi_1}{\circ}\!\equiv\!\equiv\!\overset{\phi_2}{\circ}$; $(\lambda_1, \lambda_1) = 3$, $(\lambda_2, \lambda_2) = 1$, $(\lambda_1, \lambda_2) = -\frac{3}{2}$;

(3) Fundamental Cartan integers: $\phi_1(\lambda_1) = \phi_2(\lambda_2) = 2$, $\phi_1(\lambda_2) = -1$, $\phi_2(\lambda_1) = -3$;

(4) Positive roots (in lexicographic order): $3\phi_1 + 2\phi_2$ (dominant),

$$3\phi_1 + \phi_2, 2\phi_1 + \phi_2, \phi_1 + \phi_2, \phi_1, \phi_2;$$

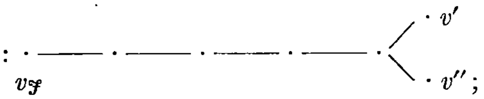
corresponding translations:

$$\lambda_1 + 2\lambda_2, \lambda_1 + \lambda_2, 2\lambda_1 + 3\lambda_2, \lambda_1 + 3\lambda_2, \lambda_1, \lambda_2;$$

norm-squares of these translations: 1, 1, 3, 3, 3, 1;

(5) $$m_2 = 5;$$

graph Φ_5:



singular planes p attached to the edges of Φ_5 (in order): $(3\phi_1 + 2\phi_2, 1)$, $(3\phi_1 + \phi_2, 1)$, $(2\phi_1 + \phi_2, 1)$, $(3\phi_1 + 2\phi_2, 2)$; $(3\phi_1 + \phi_2, 2)$ (to v'), $(\phi_1 + \phi_2, 1)$ (to v'');

beginning of the fundamental chamber:

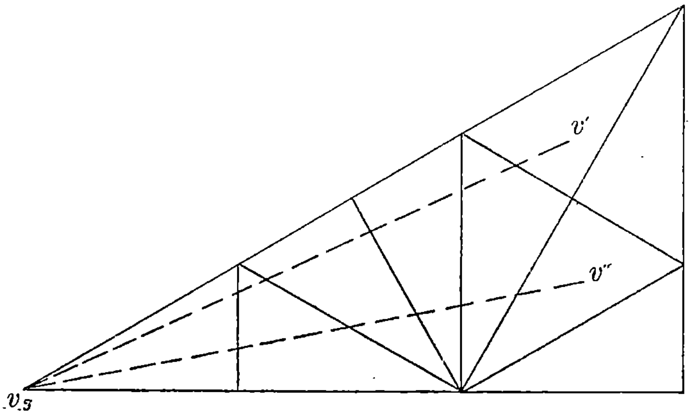


Figure 3.

As before in nos. 9 and 11, we denote by η the generator of $H^2(\Omega(G_2))$, defined by $\eta(y_{G_2}) = 1$. Our first aim is the following partial description of $H^*(\Omega(G_2); \boldsymbol{Z}_3)$.

PROPOSITION 14.1. *The element* η^3 *of* $H^6(\Omega(G_2))$ *is divisible exactly by* 3. *Put* $u = \eta^3/3$. *Then a basis for* $\sum_0^{10} H^i(\Omega(G_2); \boldsymbol{Z}_3)$ *is given by* $\{1; \eta; \eta^2; u; u\cdot\eta; u\cdot\eta^2, P^1u\}$; *here the image of* η *etc. under the coefficient reduction* $\boldsymbol{Z} \to \boldsymbol{Z}_3$ *is again denoted by* η *etc.*; *and* P^1 *is the Steenrod power that send* $H^i(X; \boldsymbol{Z}_3)$ *into* $H^{i+4}(X; \boldsymbol{Z}_3)$.

Remark. The fact that η^3 is divisible exactly by 3, is responsible for the complexity of the problem of finding $\pi_{10}(G_2) \otimes \boldsymbol{Z}_3$. From now on we write Ω for $\Omega(G_2)$. We shall prove Proposition 14.1 by considering the two G_2-cycles Γ', Γ'' attached, by (9.1), to the cells Δ', Δ''. [A part of the result, in fact all except the determination of P^1u, follows also, for instance, from the fact that, G_2 having only two-torsion, $H^*(\Omega;\mathbf{Z}_3)$ is a divided polynomial ring.] We denote by f', f'' the maps of Γ', Γ'' into Ω, defined in Chapter I, (5.4).

Γ': The variables $x_1, \cdots, x_5$, generating $H^*(\Gamma')$, correspond, in order, to the roots $3\phi_1+\phi_2$, $3\phi_1+2\phi_2$, $2\phi_1+\phi_2$, $3\phi_1+\phi_2$, $3\phi_1+2\phi_2$. The relations are given by

$$\begin{aligned} &x_1{}^2=0,\\ &x_2(x_2+x_1)=0,\\ &x_3(x_3+x_2+x_1)=0,\\ &x_4(x_4+3x_3+x_2+2x_1)=0,\\ &x_5(x_5+x_4+3x_3+2x_2+x_1)=0. \end{aligned} \tag{14.2}$$

As an example, $a_{43}=(3\phi_1+\phi_2)(2\lambda_1+3\lambda_2)=6\phi_1(\lambda_1)+9\phi_1(\lambda_2)+2\phi_1(\lambda_1)+3\phi_2(\lambda_2)=12-9-6+6=3$. The multiplicities n_i of 11.2 are given by 2, 2, 1, 1, 1, and the weights $(\tau_i,\tau_i)/(\tau_\mu,\tau_\mu)$ by 1, 1, 3, 1, 1, so that

$$a'=f'^*(\eta)=2x_1+2x_2+3x_3+x_4+x_5.$$

The following computations are facilitated by making the change of basis.

$$\begin{aligned} a'&=2x_1+2x_2+3x_3+x_4+x_5,\\ b'&=2x_1+2x_2+3x_3+x_4,\\ c'&=x_3,\\ d'&=x_1+x_2,\\ e'&=x_1. \end{aligned}$$

This transforms the relations into

$$\begin{aligned} a'^2&=a'b'+a'e'-b'e',\\ b'^2&=3(b'c'+b'd'-c'd'+c'e')-b'e',\\ c'^2&=-c'd',\\ d'^2&=d'e',\\ e'^2&=0. \end{aligned} \tag{14.3}$$

One clearly has $a'b'c'd'e'=x_1x_2x_3x_4x_5$. One computes

$$(a')^3=3(a'-e')(b'c'+b'd'-c'd'+c'e') \tag{14.4}$$

and, with $u'=(a')^3/3$,

$$u'(a')^2=4a'b'c'd'e'. \tag{14.5}$$

Γ'': The variables $x_1, \cdots, x_5$ in $H^2(\Gamma'')$ correspond to the roots $\phi_1 + \phi_2$, $3\phi_1 + 2\phi_2$, $2\phi_1 + \phi_2$, $3\phi_1 + \phi_2$, $3\phi_1 + 2\phi_2$. The relations are computed to be

$$\begin{aligned} &x_1{}^2 = 0, \\ &x_2(x_2 + 3x_1) = 0, \\ &x_3(x_3 + x_2 + x_1) = 0, \\ &x_4(x_4 + 3x_3 + 2x_2) = 0, \\ &x_5(x_5 + x_4 + 3x_3 + 2x_2 + 3x_1) = 0. \end{aligned} \tag{14.6}$$

The multiplicities n_i of are $1, 2, 1, 1, 1$; the weights $(\tau_i, \tau_i)/(\tau_\mu, \tau_\mu)$ are $3, 1, 3, 1, 1$, so that

$$a'' = f''^*(\eta) = 3x_1 + 2x_2 + 3x_3 + x_4 + x_5.$$

We change variables according to

$$\begin{aligned} a'' &= 3x_1 + 2x_2 + 3x_3 + x_4 + x_5, \\ b'' &= 3x_1 + 2x_2 + 3x_3 + x_4, \\ c'' &= x_1 \qquad\quad + x_3, \\ d'' &= \qquad\quad x_2, \\ e'' &= x_1. \end{aligned}$$

The relations go over into

$$\begin{aligned} a''^2 &= a''b'', \\ b''^2 &= 3(b''c'' + b''e'' + b''d'' - c''d'' - 3c''e''), \\ c''^2 &= -c''d'' + c''e'' + d''e'', \\ d''^2 &= -3d''e'', \\ e''^2 &= 0. \end{aligned} \tag{14.7}$$

One computes that

$$a''^3 = 3a''(b''c'' + b''e'' + b''d'' - c''d'' - 3c''e''). \tag{14.8}$$

From (14.4) and (14.8), we conclude, by (9.2), that η^3 is divisible exactly by 3; let $\eta^3/3 = u$, and $a''^3/3 = u''$. We reduce now the coefficients in $H^*(\Gamma'')$ from $\mathbf{Z}$ to $\mathbf{Z}_3$. We have then

$$u''a''^2 = (a'')^3(b''c'' + \cdots) = 0 \text{ in } H^*(\Gamma''; \mathbf{Z}_3), \tag{14.9}$$

since $(a'')^3$ is zero mod 3.

Utilizing the fact that the Steenrod power P^1 is a derivation (Cartan formula), and that P^1 applied to a two-dimensional element yields the third power of the element, we obtain after a short computation

$$P^1u'' = -a''b''c''d''e''. \tag{14.10}$$

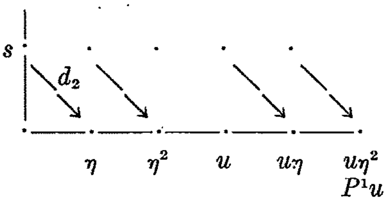
From (14.5) and (14.10), we conclude that $u\cdot\eta^2$ and P^1u are non-zero elements of $H^{10}(\Omega;\mathbf{Z}_3)$, since they map into non-zero elements under f', resp. f''. From (14.9) and (14.10), we conclude, applying f'', that $u\cdot\eta^2$ and P^1u are linearly independent. Since $H^{10}(\Omega;\mathbf{Z}_3)\approx\mathbf{Z}_3+\mathbf{Z}_3$, this proves (14.1).

15. The 3-component of $\pi_{10}(G_2)$. We compute $\pi_i(\Omega)\otimes\mathbf{Z}_3$, $i\leqq 9$, by a straightforward application of the method of killing homotopy groups, the principles of which we assume known. Let β denote the Bokstein operator $\beta\colon H^i(X;\mathbf{Z}_3)\to H^{i+1}(X;\mathbf{Z}_3)$, derived from the coefficient sequence

$$0\to\mathbf{Z}_3\to\mathbf{Z}_9\to\mathbf{Z}_3\to 0.$$

Throughout this section, $H^i(X)$ will mean $H^i(X;\mathbf{Z}_3)$. We utilize known facts about the cohomology of the Eilenberg-MacLane spaces $K(\mathbf{Z}_3,n)$, including the behavior of the Bokstein operator.

We kill $\pi_2(\Omega)$ by a suitable bundle X_1, over Ω, with $K(\mathbf{Z},1)$ or S_1 (the circle) as a fiber. The E_2-term of the corresponding spectral sequence is $H^*(\Omega)\otimes H^*(S_1)$. Let s denote the generator of $H^1(S_1)$ that maps into η under d_2. We have then $d_2(\eta\otimes s)=\eta^2$, $d_2(\eta^2\otimes s)=0$, $d_2(u\otimes s)=u\cdot\eta$, $d_2(u\cdot\eta\otimes s)=u\cdot\eta^2$.



It follows that $H^*(X_1)$, up to dimension 10, has the set $\{1,x,v,P^1v\}$ as basis, where $\dim x=5$, and where v is the image of the element u of $H^6(\Omega)$ under the projection $X_1\to\Omega$.

Furthermore the relation

$$\beta(x)=\pm v$$

holds. This follows from the fact that, using the integers as coefficients in the above computation, we have $d_2(\eta^2\cdot s)=3u$, so that the integral element v', whose reduction mod 3 yields v, satisfies $3v'=0$.

We now kill x by constructing a suitable bundle X_2 over X_1, with $K(\mathbf{Z}_3,4)$ as fiber. Let y be the generating class of $K(\mathbf{Z}_3,4)$; the cohomology of $K(\mathbf{Z}_3,4)$, up to dimension 9, is given by the basis $\{1, y, \beta y, y^2, P^1y, \beta P^1y, P^1\beta y, y\cdot\beta y\}$. In the spectral sequence of $X_2 \to X_1$, we have $E_2 = H^*(X_1) \otimes H^*(K(\mathbf{Z}_3, 4)) = E_5$, and $d_5(y) = x$. It follows that

$$d_6(\beta y) = v, d_5(y^2) = 2x \otimes y, d_5(P^1y) = \cdots = d_9(P^1y) = 0,$$
$$d_5(y\cdot\beta y) = x \otimes \beta y, d_{10}(P^1\beta y) = P^1v, d_{10}(\beta P^1y) = 0.$$

(Note that βy and P^1y are transgressive, since y is.)

One computes thus that in E_∞ the only elements of dimension $\leqq 9$ are the linear combinations of the elements $1, \bar{w}, \bar{z}$, which come from $1, P^1y, \beta P^1y$ in E_2. It follows that $H^*(X_2)$, up to dimension 9, has a basis $\{1, w, z\}$, with $\dim w = 8$, $\dim z = 9$. Moreover, $\beta w = z$, since w and z map into P^1y, βP^1y under the inclusion of the fiber $K(\mathbf{Z}_3, 4)$ in X_2.

We now kill w in $H^*(X_2)$ by constructing a suitable bundle X_3 over X_2, with fiber $K(\mathbf{Z}_3, 7)$. If t is the generating class of $H^7(\mathbf{Z}_3, 7)$, then βt generates $H^8(\mathbf{Z}\ , 7)$. In the spectral sequence we conclude from $d_8t = w$ and $d_9(\beta t) = \beta w = z$ that $H^i(X_3) = 0$ for $0 < i \leqq 9$.

From the values of the first non-trivial cohomology groups (in positive dimensions) of Ω and the X_i, $i = 1, 2, 3,$, we read off:

$$\pi_i(\Omega) \otimes \mathbf{Z}_3 = \mathbf{Z}_3 \text{ for } i = 2, 5, 8,$$
$$= 0 \text{ for the other } i\text{-values} \leqq 9.$$

Since $\pi_i(\Omega) \approx \pi_{i+1}(G_2)$, this implies in particular $\pi_{10}(G_2) \otimes \mathbf{Z}_3 = 0$, and Theorem V(d) is proved.

Chapter IV. Applications to Symmetric Spaces.

1. **Introduction.** In Chapter II, three actions were shown to be variationally complete for a symmetric pair (G, K): a) $K \times K$ on G, b) K on G/K, c) K on $\mathfrak{p}$ (by the adjoint action). In this chapter, we study some immediate consequences of Theorem I for these situations. Actually the cases a) and b) are equivalent in the following sense (this has appeared already in Chapter II, no. 6): Let $p\colon G \to G/K$ be the natural projection. If N' is a $K \times K$-orbit in G, then $N = p(N')$ is a K-orbit in G/K. Let R' be a point in G, and put $R = p(R')$. The map p induces a map p' of the path space $\Omega(G; R', N')$ (cf. Chapter I, no. 2) into $\Omega(G/K; R, N)$. It follows easily from the covering homotopy theorem for the fibering $G \to G/K$, that p' induces an isomorphism of the homotopy and therefore also of the homology of the two spaces.

By Theorem I, the mod 2 homology of $\Omega(G;R',N')$ is completely determined by the set $S=S(G;R',N')$ of transversal geodesics from R' to N' in G, as graded by the index δ_S. Our aim is to describe S and δ in each case in terms of invariants of (G,K). As we will show, the diagram of the symmetric pair (G,K) in the sense of E. Cartan [9], a variant of the diagram of a Lie group, contains all the pertinent information. Since there is no description of this diagram in the current literature, we reprove certain of Cartan's results. In particular, we have included Hunt's version of the proof of the conjugacy of the maximal tori of a symmetric space.

Properly understood, all the notions associated with the diagram of a Lie group generalize to the diagram of a symmetric space.

We will start with the adjoint action of K on $\mathfrak{p}$. Here the space $\Omega(\mathfrak{p};R,N)$ is homotopic to the orbit N. Our formulas therefore describe the homology of the orbits of K in $\mathfrak{p}$.

2. The adjoint action of K on $\mathfrak{p}$.

We recall the pertinent definitions from Chapter II. The $(+1)$-eigen space of $*$ is the Lie algebra $\mathfrak{k}$ of K; its orthogonal complement, the (-1)-space of $*$, is $\mathfrak{p}$. Thus $\mathfrak{g}=\mathfrak{k}\oplus\mathfrak{p}$. For any $A\in\mathfrak{g}$, we have $\mathfrak{g}_A=\{X:[A,X]=0\}$; $\mathfrak{p}_A=\mathfrak{g}_A\cap\mathfrak{p}$; $\mathfrak{k}_A=\mathfrak{g}_A\cap\mathfrak{k}$.

PROPOSITION 2.1. *For any $A\in\mathfrak{p}$, the equations*

$$\text{(a)}\qquad \mathfrak{g}_A=\mathfrak{k}_A\oplus\mathfrak{p}_A$$

$$\text{(b)}\qquad \mathfrak{p}=[\mathfrak{k},A]\oplus\mathfrak{p}_A$$

represent orthogonal decompositions.

Relation (2.1(a)) follows from Chapter V, 3.1; for (2.1(b)), we use Chapter II, (7.5), with A replaced by zero and X replaced by A.

Let $\mathfrak{g}_A{}^{\perp}$ denote the orthogonal complement of $\mathfrak{g}_A$ in $\mathfrak{g}$. We see from (2.1(a)) and (2.1(b)) that $[\mathfrak{k},A]=\mathfrak{g}_A{}^{\perp}\cap\mathfrak{p}$, and that ad$A$ maps $\mathfrak{g}_A{}^{\perp}\cap k$ isomorphically onto $\mathfrak{g}_A{}^{\perp}\cap\mathfrak{p}$, so that these two spaces have the same dimension. We conclude that

$$\text{(2.2)}\qquad \dim\mathfrak{k}_A-\dim\mathfrak{p}_A=\dim\mathfrak{t}-\dim\mathfrak{p},$$

independent of A.

This can also be expressed by saying that the trace of $*$ on $\mathfrak{g}_A$ equals the trace of $*$ on $\mathfrak{g}$, for any A.

DEFINITION 2.3. *A maximal abelian subalgebra of $\mathfrak{p}$ is called a Cartan algebra of (G,K). If $\mathfrak{t}$ is such an algebra, $A\in\mathfrak{t}$ is called a general point of $\mathfrak{t}$ if $\mathfrak{p}_A=\mathfrak{t}$. The dimension of $\mathfrak{t}$ is called the rank of (G,K).*

It is clear from general theory that Cartan algebras as well as general points on them exist. In the following, we *denote by* $\mathfrak{t}$ *a fixed Cartan algebra of* (G,K), *and let* A *be a fixed general point of* $\mathfrak{t}$.

Let Q be a point of $\mathfrak{p}$, and let N be the K-orbit of Q. As in Chapter I, no. 2, we denote by $S(\mathfrak{p};A,N)$ the set of geodesics (i.e. straight line segments in $\mathfrak{p}$) which are transversal to the action of K on $\mathfrak{p}$ and join A to points of N. Let $S(\mathfrak{t};A,\mathfrak{t}\cap N)$ be the set of straight lines in $\mathfrak{t}$ joining A to points of $\mathfrak{t}\cap N$.

PROPOSITION 2.4. $S(\mathfrak{p};A,N)=S(\mathfrak{t};A,\mathfrak{t}\cap N)$.

Proof. A transversal line from A to N must be perpendicular to the orbit of A at A (cf. Chapter I, (2.2)). By Chapter II, (7.1) and (7.4), the orthogonal complement to the orbit of A, at A, is precisely $\mathfrak{p}_A$, which is equal to $\mathfrak{t}$. Hence all the elements of $S(\mathfrak{p};A,N)$ lie in $\mathfrak{t}$. Conversely, every line in $\mathfrak{t}$ starting at A is transversal. This proves the proposition.

COROLLARY 2.5. *Every orbit* N *of* K *on* $\mathfrak{p}$ *intersects* $\mathfrak{t}$.

Because every such orbit is compact, there must be a point at which N is closest to A. The line from A to that point will then have to be transversal. Hence $S(\mathfrak{p};A,N)$ is not empty. Now apply Proposition 2.4.

COROLLARY 2.6. *Any two Cartan algebras of* (G,K) *are conjugate under the adjoint action of* K.

Proof. Let $\mathfrak{t}'$ be any Cartan algebra of (G,K), let B be a general point of $\mathfrak{t}'$ and let N be the orbit of B. Since $N\cap\mathfrak{t}\neq 0$ there exists a $k\in K$, such that $\mathrm{Ad}k\cdot B\subset\mathfrak{t}$. But then clearly $\mathrm{Ad}k\cdot\mathfrak{t}'=\mathfrak{t}$, so that $\mathfrak{t}'$ is conjugate to $\mathfrak{t}$.

Note. This corollary goes back to E. Cartan [9]. The proof given here is an immediate extension of the proof due to Hunt for the conjugacy of Cartan algebras in the group case [13].

PROPOSITION 2.7. (a) *Every orbit of* K *in* $\mathfrak{p}$ *intersects* $\mathfrak{t}$ *orthogonally.* (b) *The orbit through* A *has maximal dimension.*

Proof. Clearly $\mathfrak{p}_B\supset\mathfrak{p}_A=\mathfrak{t}$ for any $B\in\mathfrak{t}$. As the transversal space to the orbit through B is $\mathfrak{p}_B$, this inclusion together with Corollary 2.5 proves both statements.

We write δ_K' for the defect function of the adjoint action of K on $\mathfrak{p}$, as defined in Chapter I, (7.4). Because of (2.7(b)) and Chapter II, (7.1), we have

$$\delta_K'(B)=\dim[\mathfrak{k},A]-\dim[\mathfrak{k},B]. \tag{2.8}$$

Applying (2.1(b)), (2.2), we obtain

$$\delta_K'(B) = \dim \mathfrak{p}_B - \dim \mathfrak{p}_A = \dim \mathfrak{k}_B - \dim \mathfrak{k}_A.$$

This proves

PROPOSITION 2.9.

$$\delta_K'(B) = \tfrac{1}{2}(\dim \mathfrak{g}_B - \dim \mathfrak{g}_A)$$

for any $B \in \mathfrak{p}$.

According to Chapter I, (7.3), the defect δ_s of any segment

$$s \in S(\mathfrak{t}; A, N \cap \mathfrak{t}),$$

with end points A and Q, is given by

$$\delta_s = \sum_{0 \leqq \alpha < 1} \delta_K'((1-\alpha)A + \alpha Q). \tag{2.10}$$

We extend $\mathfrak{t}$ to a Cartan algebra $\tilde{\mathfrak{t}}$ of the Lie algebra $\mathfrak{g}$, and denote by $D'(G)$ the infinitesimal diagram of G on $\tilde{\mathfrak{t}}$ (cf. Chapter III, no. 1).

As a consequence of (2.9), δ_K' can be described entirely in terms of $D'(G)$. In fact, it is easily seen that

(2.11) $\delta_K'(B) =$ *number of planes of* $D'(G)$ *containing* B, *but not containing all of* $\mathfrak{t}$.

(For each root $\theta \in \mathfrak{R}$ with $\theta(B) = 0$, the dimension of $\mathfrak{g}_B$ goes up by two.)

The set of points B in $\mathfrak{t}$ with $\delta_K'(B) > 0$ is called the infinitesimal diagram of (G, K), and is denoted by $D'(G, K)$; it consists of a finite number of planes through the origin. The defect δ_s of a segment s is the number of planes, properly weighted, in $D'(G, K)$ crossed by s; note that planes of $D'(G, K)$ containing the end point Q of s do not count in δ_s.

The connected components of the complement of $D'(G, K)$ in $\mathfrak{t}$ are called the *fundamental chambers* of $D'(G, K)$. In complete analogy to the group case, every chamber $\mathfrak{F}$ plays the role of a fundamental domain for the Weyl group of (G, K), as will be seen later. This group, denoted by $\mathfrak{W}(G, K)$, is defined as the quotient of the group consisting of the elements in K which keep $\mathfrak{t}$ setwise fixed (the normalizer of $\mathfrak{t}$) modulo the group of the elements which keep $\mathfrak{t}$ pointwise fixed (i.e. $K_{\mathfrak{t}}$). From Proposition 2.7(a), applied to A (and the fact that all orbits are compact), it follows that $\mathfrak{W}(G, K)$ is a finite group. It is also clear that if B is any general point of $\mathfrak{t}$ and N is the orbit of B, then

(2.12) $N \cap \mathfrak{t} =$ *orbit of* B *under* $\mathfrak{W}(G, K)$.

(Actually, a more general statement is true: if A, B are two subsets of $\mathfrak{t}$, conjugate under $k \in K$, then there exists an element of the Weyl group, whose restriction to A equals that of $\mathrm{Ad}k$. One proves this by considering the centralizer, in G, of $\mathfrak{t} \cap \mathrm{Ad}k(\mathfrak{t})$. A similar statement holds for the global case, i. e., for the operation of the Weyl group on the maximal torus T, cf. Definition 3. 3.)

For any K-orbit N on $\mathfrak{p}$, we write $\bar{S}_*(N)$ for the graded $\mathbf{Z}_2$-vector space generated by the elements of $S(\mathfrak{t}; A, \mathfrak{t} \cap N)$, the dimension of a segment being the defect δ_s (cf. (2. 10)).

We can now state the consequences of Theorems I and II in the following form:

THEOREM VI. *Let N be any orbit of K on $\mathfrak{p}$. Then (as graded modules)*

$$H_*(N; \mathbf{Z}_2) \approx \bar{S}_*(N).$$

Proof. We have $\Omega(\mathfrak{p}; A, N) \approx N$ because $\mathfrak{p}$ is a Euclidean space (cf. Chapter III, no. 6). By Theorem II, the action of K on $\mathfrak{p}$ is variationally complete, and the point A has defect 0. Hence Theorem I is applicable, and describes $H_*(N; \mathbf{Z}_2)$ in terms of $S(\mathfrak{p}; A, N)$, or, because of (2. 4), in terms of $S(\mathfrak{t}; A, \mathfrak{t} \cap N)$, graded by δ_s.

Remarks. This theorem is the complete analogue of Theorem III in [6], except that the coefficients have been reduced mod 2. One can of course give the data for $\bar{S}_*(N)$ entirely in terms of the roots of G, and the group $\mathfrak{W}(G, K)$. Such a formulation was given in [6]. We omit these details here, and give only one example in the next corollary.

COROLLARY 2. 13. *Let $\mathfrak{W}_*$ be the graded $\mathbf{Z}_2$-vector space generated by the elements of $\mathfrak{W}(G, K)$, the dimension of $w \in \mathfrak{W}(G, K)$ being*

$$\sum_{0<\alpha\leqq 1} \delta_K'\{(1-\alpha)A + \alpha(w \cdot A)\}.$$

Let $K_{\mathfrak{t}}$ be the centralizer of $\mathfrak{t}$ in K. Then as graded modules,

$$H_*(K/K_{\mathfrak{t}}; \mathbf{Z}_2) = \mathfrak{W}_*$$

Proof. The elements of $\mathfrak{W}(G, K)$ clearly permute the fundamental chambers of $D'(G, K)$, since the function δ_K' is invariant under $\mathfrak{W}(G, K)$. We need the following proposition:

PROPOSITION 2. 14. *The Weyl group $\mathfrak{W}(G, K)$ is transitively and faithfully represented by the permutations it induces in the fundamental chambers of $D'(G, K)$.*

We prove this proposition by means of Theorem VI. Let $\mathfrak{F}$ be any fundamental chamber of $D'(G,K)$, and let B be a general point in it with K-orbit N. Let $\mathfrak{F}_A$ be the chamber that contains A. By (2.10), (2.11), (2.12), the number of points in the $\mathfrak{W}(G,K)$-orbit of B that lie in $\mathfrak{F}_A$ equals the number of segments in $S(\mathfrak{t};A,\mathfrak{t}\cap N)$ of index 0. By Theorem VI, this is also the number of components of N. But K being connected, N is connected, and (2.14) is proved.

The Corollary 2.13 is now immediate. Let B be taken in $\mathfrak{F}_A$. With any $w\in\mathfrak{W}(G,K)$, associate the segment from A to $w\cdot B$. This induces a gradation preserving isomorphism of $\bar{S}_*(N)$ and $\mathfrak{W}_*$. Since B is general in $\mathfrak{t}$, its K-orbit N is homeomorphic to $K/K_{\mathfrak{t}}$. The corollary follows now from Theorem VI.

Let $\mathfrak{t}'$ be any subspace of $\mathfrak{t}$. A result analogous to (2.13) can then be stated for the homology of $K/K_{\mathfrak{t}'}$ in terms of the quotient set of $\mathfrak{W}(G,K)$ by the subgroup that leaves $\mathfrak{t}'$ point-wise fixed.

3. The action of $K\times K$ on G. This section is the global analogue of the previous one. As in Chapter II, we write $\mathfrak{k}_a=\mathfrak{k}\cap\mathrm{Ad}\,a^{-1}\mathfrak{k}$, $\mathfrak{p}_a=\mathfrak{p}\cap\mathrm{Ad}\,a^{-1}\mathfrak{p}$ for any $a\in G$. We also write $\mathfrak{g}_a$ for $\{X\in g\colon \mathrm{Ad}\,aX=X\}$; note that the definition of $\mathfrak{g}_a$ differs from that of $\mathfrak{k}_a$ and $\mathfrak{p}_a$.

PROPOSITION 3.1. *If* $a^*=a^{-1}$, *then*

(a) $$\mathfrak{g}_{a^2}=\mathfrak{k}_a\oplus\mathfrak{p}_a$$

(b) $$\mathfrak{p}=\{\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1}\}\,\mathfrak{k}\oplus\mathfrak{p}_a$$

are orthogonal decompositions.

Proof. Clearly, $\mathfrak{g}_{a^2}$ is stable under *. Hence $\mathfrak{g}_{a^2}=\mathfrak{g}_{a^2}\cap\mathfrak{k}+\mathfrak{g}_{a^2}\cap\mathfrak{p}$. If $Z\in\mathfrak{p}_a$, then $\mathrm{Ad}\,aZ\in\mathfrak{p}$. Hence, applying *, $\mathrm{Ad}\,a^{-1}Z=\mathrm{Ad}\,aZ$, whence $Z\in\mathfrak{g}_{a^2}\cap\mathfrak{p}$. Hence $\mathfrak{p}_a\subset\mathfrak{g}_{a^2}\cap\mathfrak{p}$. Conversely, if $Z\in\mathfrak{g}_{a^2}\cap\mathfrak{p}$, then $(\mathrm{Ad}\,a^{-1}Z)^*=-\mathrm{Ad}\,aZ=-\mathrm{Ad}\,a^{-1}Z$, so that $Z\in\mathfrak{p}_a$. Hence $\mathfrak{p}\supset\mathfrak{g}_{a^2}\cap\mathfrak{p}$. Quite similarly, one finds that $\mathfrak{g}_{a^2}\cap\mathfrak{k}=\mathfrak{k}_a$. This proves 3.1(a). Next, $\{(\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1})Z\}^*=-(\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1})Z^*$. Hence, $(\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1})\mathfrak{k}\subset\mathfrak{p}$, and $(\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1})\mathfrak{p}\subset\mathfrak{k}$. Suppose that $Z\in\mathfrak{p}$ is perpendicular to $(\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1})\mathfrak{k}$, so that

$$(\{\mathrm{Ad}\,a-\mathrm{Ad}\,a^{-1}\}\mathfrak{k},Z)=0.$$

This implies $(\mathrm{Ad}\,a^{-1}-\mathrm{Ad}\,a)Z\in\mathfrak{p}$, whence $\mathrm{Ad}\,a^{-1}Z=\mathrm{Ad}\,aZ$, so that $Z\in\mathfrak{g}_{a^2}\cap\mathfrak{p}=\mathfrak{p}_a$. The argument can be reversed, and (3.1(b)) is proved.

COROLLARY 3.2. *If* $a^*=a^{-1}$, then

$$\dim \mathfrak{g}_{a^2} \cap \mathfrak{p} = \dim \mathfrak{g}_{a^2} \cap \mathfrak{k};$$

$$\dim \mathfrak{k}_a - \dim \mathfrak{p}_a = \dim \mathfrak{k} - \dim \mathfrak{p}.$$

This follows from (3.1(a), (b)) as (2.2) followed from (2.1(a), (b)) in no. 2; first one has to verify, using *, that $\mathfrak{k}_a$ is the kernel of the restriction of $\mathrm{Ad}a - \mathrm{Ad}a^{-1}$ to $\mathfrak{k}$.

DEFINITION 3.3. *The image in G, under the exponential map, of a Cartan algebra $\mathfrak{t}$ of (G, K) is called a maximal torus of (G, K), and is denoted by T. The point $a \in T$ is called general if $\mathfrak{p}_a = \mathfrak{t}$.*

The maximality of $\mathfrak{t}$ implies that $\exp \mathfrak{t}$ is closed in G. By general theory, we can find an $a \in T$ such that $\mathfrak{g}_{a^2} \cap \mathfrak{p} = \mathfrak{t}$. Hence by (3.1), T contains general points.

In the sequel, T denotes a fixed maximal torus of (G, K) and a is a fixed general point of T. The tangent space to T at the identity is identified with the Cartan algebra $\mathfrak{t}$.

Let $b \in T$, and let $N = K \cdot b \cdot K$ be the orbit of b under $K \times K$. By Chapter II, (7.1), (7.4) the transversal space to N at b is precisely $b \cdot \mathfrak{p}_b$. The arguments of no. 2 therefore easily yield the following analogue of (2.4), (2.5), and (2.7).

PROPOSITION 3.4. *Let N be any orbit of $K \times K$ on G. Then $N \cap T$ is not vacuous. N intersects T orthogonally (and therefore at a finite number of places). The sets*

$$S(G; a, N) \text{ and } S(T; a, T \cap N)$$

coincide. The orbit of a has maximal dimension.

Here $S(G; a, N)$ of course denotes the set of transversal geodesics from a to N, while $S(T; a, T \cap N)$ stands for the, automatically transversal, geodesics on T from a to points of $N \cap T$.

We denote by δ_K the defect function of $K \times K$ on G, defined as in Chapter I, (7.1). By Chapter II, no. 3 we have $\delta_K(b) = \dim \mathfrak{k}^a - \dim \mathfrak{k}^b$. As in no. 2, one proves that

$$\delta_K(b) = \tfrac{1}{2}(\dim \mathfrak{g}_{b^2} - \dim \mathfrak{g}_{a^2}) \text{ for any } b \in T. \tag{3.5}$$

(Note that for such b's the relation $b^* = b^{-1}$ holds.)

As before, $\bar{\mathfrak{t}}$ is a Cartan algebra of $\mathfrak{g}$, containing $\mathfrak{t}$; let $D(G)$ be the diagram of G on $\bar{\mathfrak{t}}$ (cf. Chapter III, no. 1). We define the *defect function* δ of (G, K) by

(3.6) $\delta(B) =$ *number of planes of* $D(G)$ *that contain* B, *but do not contain all of* $\mathfrak{t}$, *for any* $B \in \mathfrak{t}$.

The diagram $D(G,K)$ consists now by definition of all $B \in \mathfrak{t}$ with $\delta(B) > 0$; it can also be described as the union of the intersections $\mathfrak{p} \cap \mathfrak{t}$ for all those singular planes $p = (\theta, n) \in \mathfrak{P}$, whose translation vector τ_θ is not orthogonal to $\mathfrak{t}$.

The defects δ and δ_K are related by the following proposition.

PROPOSITION 3.7. *Let* $\rho\colon \mathfrak{t} \to T$ *be defined by* $\rho(B) = \exp(\frac{1}{2}B)$. *Then* $\delta_K \circ \rho = \delta$, *where* δ_K *is the defect function of* $K \times K$ *on* G, *and* δ *is the defect function of* $D(G,K)$.

This formula is an immediate consequence of (3.5), and the meaning of $D(G)$ for the stabilizers of points in T. Let A be an element of $\mathfrak{t}$ that maps into a under ρ; clearly A is general in $\mathfrak{t}$. For any $K \times K$-orbit N, the elements of $S(T; a, T \cap N)$ then lift under ρ uniquely into straight line segments in $\mathfrak{t}$, with initial point A. Let $S'(N) = S'(\mathfrak{t}; A, \rho^{-1}(T \cap N))$ denote this set of line segments. Let s', with end points A and B, be an element of $S'(N)$, corresponding to $s \in S(T; a, T \cap N)$. Then the δ_K-defect of s is equal to the δ-defect of s', given by

$$\delta_{s'} = \sum_{0 \leq \alpha < 1} \delta((1-\alpha)A + \alpha B), \tag{3.8}$$

the number of planes, properly weighted, of $D(G,K)$ crossed by s'. Finally, let $S'_*(N)$ be the $\mathbf{Z}_2$-vector space generated by $S'(N)$ according to the defect δ. The global analogue of Theorem VI now clearly takes the following form:

THEOREM VII. *Let* N *be any orbit of* $K \times K$ *on* G. *Then, as graded modules,*

$$H_*\{\Omega(G; a, N); \mathbf{Z}_2\} \approx S'_*(N).$$

The Corollary 2.13 to Theorem VI also has a global analogue. We will formulate it in terms of the cells of $D(G,K)$. By definition, these are the connected components of $\mathfrak{t} - D(G,K)$. We let $\mathfrak{F}$ be a fundamental chamber of $D'(G,K)$ and denote by $\{\Delta\}_{\mathfrak{F}}$ the set of cells of $D(G,K)$ contained in the closure of $\mathfrak{F}$. We assign an index $\delta(\Delta)$ to $\Delta \in \{\Delta\}_{\mathfrak{F}}$ by the formula

$$\delta(\Delta) = \sum_{0 < t \leq 1} \delta(tB), \tag{3.9}$$

where δ is the defect function of (G,K) and B is any point of Δ. (In words, $\delta(\Delta) =$ number of properly counted planes in $D(G,K)$ crossed by a line from 0 to a point of Δ.) Finally, we let $\mathfrak{J}_*$ be the graded $\boldsymbol{Z}_2$-vector space generated by $\{\Delta\}_{\mathfrak{J}}$ and graded by δ.

COROLLARY 3.10. *Let* $\pi_1(G)=0$. *Then,*

$$H_*(\Omega(G/K);\boldsymbol{Z}_2)\approx\mathfrak{J}_*$$

as graded modules.

Proof. Because $\pi_1(G)=0$ and $\pi_0(K)=0$, G/K is simply connected. Hence $\Omega(G/K)$ has precisely one component. Let $N=K$ be the orbit of $e\in G$ under $K\times K$. Then, as explained in no. 1, $\Omega(G/K)$ can be identified with $\Omega(G;a,K)$. Let $\mathfrak{J}_0=\rho^{-1}(K\cap T)$, so that $S'(K)$ consist of the segments from A to the points of $\mathfrak{J}_0$. Then Theorem VII implies that $\mathfrak{J}_0$ intersects the closure of any cell Δ in $D(G,K)$ precisely once. To show this, we may assume $A\in\Delta$. Since $\Omega(G;a,K)$ is connected, by Theorem VII there is only one segment in $S'(K)$ of index 0; but this is equivalent to the assertion about $\mathfrak{J}_0$.

Now to any $s\in S'(K)$, with second end point $B\in\mathfrak{J}_0$, there exists a unique $w\in\mathfrak{W}(G,K)$ such that $w\cdot(A-B)$ lies in the interior of a cell in $\mathfrak{J}$. As in [6], one shows that this defines a one-to-one map of $S'(K)$ onto $\{\Delta\}_{\mathfrak{J}}$, and that the induced isomorphism of $\bar{S}'_*(K)$ onto $\mathfrak{J}_*$ is gradation preserving. The Corollary now follows from Theorem VII.

As a simple application, we will prove the following proposition, which, as the referee pointed out, is contained in [9], no. 101.

PROPOSITION 3.11. *Let * be an involution of the compact, simply connected Lie group G. Then the set of fixed points of * is connected.*

Proof. Let (G,K) be the symmetric pair determined by *, and let $\hat{K}$ be the fixed point set of *. Thus K is the e-component of $\hat{K}$. We start with the following lemma.

LEMMA 3.12. *If* $K\cap T=\hat{K}\cap T$, *then* $K=\hat{K}$.

Proof. Suppose K_1 is a component of $\hat{K}$ different from K. The $K\times K$-orbit of any point e_1 of K_1 is clearly K_1 itself. By (3.4), this orbit intersects T, so that $K_1\cap T$ is not vacuous. But $K\cap T$ and $K_1\cap T$ are disjoint, and (3.12) follows. Next, we remark:

(3.13) *The set* $\hat{K}\cap T$ *consists of the points* $x\in T$, *with* $x^2=e$.

This follows from the fact that on T the involution * is just inversion.

LEMMA 3.14. *If* $\pi_1(G)=0$, *then* $K\cap T=\hat{K}\cap T$.

Proof. Let $\mathcal{J}_0 = \rho^{-1}(K \cap T)$ as before, and let $\mathcal{J} = \rho^{-1}(\hat{K} \cap T)$. It follows from (3.13) and the definition $\rho(B) = \exp(\frac{1}{2}B)$ that $\mathcal{J}$ consists of the lattice of points in $\mathfrak{t}$ which under the exponential map go into e. We shall show that $\mathcal{J}_0 = \mathcal{J}$. Suppose then that $\mathcal{J}$ is a proper refinement of $\mathcal{J}_0$. Since the closed cells of $D(G,K)$ cover $\mathfrak{t}$, and since $\mathcal{J}_0$ intersects each closed cell of $D(G,K)$ in precisely one point (as noted in the proof of 3.10), the lattice $\mathcal{J}$ will have to intersect the closure of some cell, say Δ, in at least two points. From the construction of $D(G,K)$, it is clear that Δ is contained in the closure of some cell Δ_1 of $D(G)$ in $\tilde{\mathfrak{t}}$. (Here $\tilde{\mathfrak{t}}$ is a Cartan algebra of G containing $\mathfrak{t}$.) Hence the closure of Δ_1 in $D(G)$ intersects $\mathcal{J}$ in at least two points. But it is well known that if $\pi_1(G) = 0$, then each closed cell of $D(G)$ contains exactly one point whose exponential image is e (cf. [20]). This contradiction proves (3.14). The two Lemmas 3.12, 3.14 prove Proposition 3.11.

4. An example. Symmetric spaces of maximal rank. According to (3.10), the mod 2 Poincaré series of $\Omega(G/K)$ is given by $\sum_{\mathcal{F}} t^{\delta(\Delta)}$, where Δ runs over the cells of a fundamental chamber $\mathcal{F}$ in $D(G,K)$. In Theorem B, Part 1, of [6], the Poincaré series of $\Omega(G)$ was given as $\sum_{\mathcal{F}} t^{2\lambda(\Delta)}$, where one now sums over the cells of a fundamental chamber in $D(G)$. Suppose now that the maximal torus of (G,K) is also a maximal torus of G. In this case, $D(G)$ coincides with $D(G,K)$, and $\delta(\Delta)$ as defined here, agrees with the $\lambda(\Delta)$ of [6]. We therefore get the following somewhat mysterious application of 3.10.

PROPOSITION 4.1. *Suppose that $\pi_1(G) = 0$, and that the rank of the symmetric pair (G,K) equals the rank of G. Then*

$$\dim H_q(\Omega(G/K); \mathbf{Z}_2) = \dim H_{2q}(\Omega(G); \mathbf{Z}_2).$$

Every 1-connected Lie group has an essentially unique involution *, with rank $(G,K) = \operatorname{rank} G$. This involution correspond to "the" real form of the complexified Lie group. We will call a G/K obtained in this way a symmetric space of maximal rank. The mod 2 Betti numbers of $\Omega(G/K)$ are then determined by the Betti numbers of $\Omega(G)$ by (4.1); on the other hand, the Poincaré series of $\Omega(G)$ is determined by the Poincaré polynomial of G (cf. [6]). Indeed, if

$$P(G;t) = (1 + t^{2m_1-1}) \cdots (1 + t^{2m_l-1}),$$

then

$$P(\Omega(G);t) = (1 - t^{2(m_1-1)})^{-1} \cdots (1 - t^{2(m_l-1)})^{-1}.$$

Combining this observation with (4.1), we obtain the following proposition.

PROPOSITION 4.2. *Let G/K be a symmetric space of maximal rank, where G is a 1-connected compact Lie group. If $m_1, \cdots, m_l$ are the primitive exponents of G, then*

$$P(\Omega(G/K); \mathbf{Z}_2; t) = (1-t^{m_1-1})^{-1}(1-t^{m_2-1})^{-1} \cdots (1-t^{m_l-1})^{-1}.$$

A similar comparison of (2.15) with Theorem B, Part 2 of [6], leads to the following proposition.

PROPOSITION 4.3. *Let (G,K) be a symmetric pair of maximal rank. Let T_1 be a torus of G contained in a maximal torus of (G,K). Let K_{T_1} and G_{T_1} denote the centralizers of T_1 in K and G respectively. Then*

$$\dim H_q(K/K_{T_1}; \mathbf{Z}_2) = \dim H_{2q}(G/G_{T_1}; \mathbf{Z}_2).$$

As a concrete instance of the halving in dimensions, we mention the real projective space as opposed to the complex projective space.

Applying the Hirsch formula [1] to the right hand side of (4.3), with $T_1 = T$, one obtains the following analogue of (4.2).

PROPOSITION 4.4. *Let (G,K) be a symmetric pair of maximal rank; let T be a maximal torus of (G,K); let $m_1, \cdots, m_l$ be the primitive exponents of G. Then*

$$P(K/K_T; \mathbf{Z}_2; t) = (1-t^{m_1}) \cdots (1-t^{m_l})/(1-t)^l.$$

In certain cases, for instance when $G = SU(n)$ and $K = SO(n)$, the formulas (4.3) and (4.4) also follow from Borel's work with the maximal tori mod 2 of G [2].

UNIVERSITY OF MICHIGAN.

REFERENCES.

[1] A. Borel, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[2] ———, "La cohomologie mod 2 de certains espaces homogènes," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 165-197.

[3] ———, "Sur l'homologie et la cohomologie des groupes de Lie compacts connexes," *American Journal of Mathematics*, vol. 76 (1954), pp. 273-302.

[4] ———, "Topology of Lie groups and characteristic classes," *Bulletin of the American Mathematical Society*, vol. 61 (1955), pp. 397-432.

[5] A. Borel and J. de-Siebenthal, "Les sous-groupes fermés de rang maximum des groupes de Lie clos," *Commentarii Mathematici Helvetici*, vol. 23 (1949), pp. 200-221.

[6] R. Bott, "An application of the Morse theory to the topology of Lie groups," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 251-282.

[7] R. Bott and H. Samelson, "The cohomology ring of G/T," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 490-493.

[8] ———, "Applications of Morse theory to symmetric spaces," *Proceedings of the Symposium international de Topologia Algebraica*, Mexico City, 1956, (to appear).

[9] E. Cartan, "Sur certaines formes Riemanniennes remarquables des géométries a groups fondamental simple," *Annales Scientifiques de l'Ecole Normale Supérieure*, vol. 44 (1927), pp. 345-467.

[10] H. Hopf, "Über den Rang geschlossener Lie'scher Gruppen," *Commentarii Mathematici Helvetici*, vol. 13 (1940/51), pp. 119-143.

[11] ———, "Maximale Toroide und singuläre Elemente in geschlossenen Lie'schen Gruppen," *ibid.*, vol. 15 (1942/43), pp. 59-70.

[12] ———, "Sur une formule de la théorie des espaces fibrés," *Collogue de Topologie Bruxelles* (1950), pp. 117-121.

[13] G. A. Hunt, "A theorem of Elie Cartan," *Proceedings of the American Mathematical Society*, vol. 7 (1956), pp. 307-308.

[14] S. D. Liao, "On the theory of obstructions of fiber bundles," *Annals of Mathematics*, vol. 60 (1954), pp. 146-191.

[15] D. Montgomery, H. Samelson and C. T. Yang, "Exceptional orbits of highest dimension," *Annals of Mathematics*, vol. 64 (1956), pp. 131-141.

[16] M. Morse, *The Calculus of Variations in the Large*, American Mathematical Society Colloquium Publications, vol. 18, New York, 1934.

[17] H. Seifert and W. Threlfall, *Variationsrechnung im Grossen* (*Theorie von Marston Morse*), Teubner, Leipzig, 1938.

[18] J. P. Serre, "Homologie singulière des espaces fibrés. Applications," *Annals of Mathematics*, vol. 54 (1951), pp. 425-505.

[19] N. E. Steenrod, "Cohomology operations derived from the symmetric group," *Commentarii Mathematici Helvetici*, vol. 31 (1957), pp. 195-218.

[20] E. Stiefel, "Über eine Beziehung zwischen geschlossenen Lie'schen Gruppen und diskontinuierlichen Bewegungsgruppen euklidischer Räume und ihre Anwendung auf die Aufzählung der einfachen Lie'schen Gruppen," *ibid.*, vol. 14 (1941/42), pp. 350-380.